ЦИФРОВЫЕ
ТЕХНОЛОГИИ
И ПРАВО

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

СБОРНИК НАУЧНЫХ ТРУДОВ
I МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ
КОНФЕРЕНЦИИ

В шести томах

Том 2

КИУ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ»

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

I Международная научно-практическая конференция

Как цитировать: Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 2. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 556 с. EDN: JSIXFM. DOI: http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556

For citation: Digital Technologies and Law: collection of scientific articles of the I International Scientific and Practical Conference (Kazan, September 23, 2022) / eds.: I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova. In 6 vol. Vol. 2. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2022. – 556 p. EDN: JSIXFM. DOI: http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556

Казанский
инновационный
университет имени
В. Г. Тимирясова

Министерство цифрового развития
государственного управления,
информационных технологий
и связи Республики Татарстан

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
I Международной научно-практической конференции

23 сентября 2022 г.
г. Казань

В шести томах
Том 2

Казань ■ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ■ 2022

Kazan
Innovative University
named after
V. G. Timiryasov

Ministry of Digitalization of Public
Administration, Information
Technologies and Communications
of the Republic of Tatarstan

DIGITAL TECHNOLOGIES AND LAW

Collection of scientific articles
of the I International Scientific and Practical Conference

September 23, 2022
Kazan

In 6 volumes
Volume 2

Kazan ■ "POZNANIYE" PUBLISHERS ■ 2022

УДК 004:34(063)
ББК 67с51я43
Ц75

Печатается по решению редакционно-издательского совета
Казанского инновационного университета имени В. Г. Тимирясова

Ц75 **Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции** (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 2. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 556 с. EDN: JSIXFM. DOI: http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556
ISBN 978-5-8399-0767-6
ISBN 978-5-8399-0769-0 (Том 2)

Вошедшие в сборник научные труды приурочены к Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 23 сентября в Казани в рамках Международного форума Kazan Digital Week 2022, организуемого Кабинетом Министров Республики Татарстан под эгидой Правительства Российской Федерации.

Широкий круг рассмотренных на конференции теоретико-методологических и практикоориентированных, междисциплинарных и отраслевых вопросов связан с приоритетами правового развития цифровых технологий, перспективами правового регулирования цифрового профилирования, экспериментальными и специальными правовыми режимам в сфере создания цифровых инноваций, интеллектуальными правами, трудовыми и связанными с ними отношениями, блокчейн-технологиями, криптовалютой, децентрализованными финансами в правовых реалиях, искусственным интеллектом, робототехникой и др.

Научные труды представленного тома систематизированы по современным трендам развития цифровых технологий в системе уголовно-правовых, международно-правовых и частноправовых (цивилистических) отношений.

Нашедшие отражение в этом и иных томах сборника идеи и предложения в своей совокупности являются ключом к пониманию интеллектуальной карты смыслов, которые будут интересны ученым-правоведам и экспертам в области цифровых технологий, практикующим юристам, представителям правотворческих и правоприменительных органов, государственным служащим и участникам реального сектора экономики, молодым исследователям-студентам, магистрантам и аспирантам, всем интересующимся вопросами взаимовлияния цифровых технологий и права.

УДК 004:34(063)
ББК 67с51я43

ISBN 978-5-8399-0767-6
ISBN 978-5-8399-0769-0 (Том 2)

UDC 004:34(063)
LBC 67c51я43

Published by the decision of the Editorial-Publishing Board
of Kazan Innovative University named after V. G. Timiryasov

Digital Technologies and Law: collection of scientific articles of the I International Scientific and Practical Conference (Kazan, September 23, 2022) / eds.: I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova. In 6 vol. Vol. 2. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2022. – 556 p. EDN: JSIXFM. DOI: http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556
ISBN 978-5-8399-0767-6
ISBN 978-5-8399-0769-0 (Volume 2)

The research works included into the collection are correlated with International Scientific and Practical Conference "Digital Technologies and Law" which took place on September 23 in Kazan during the International Forum Kazan Digital Week 2022, organized by the Cabinet of Ministers of the Republic of Tatarstan under the aegis of the Government of the Russian Federation.

The broad range of theoretical and methodological, practice-oriented, interdisciplinary and sectoral issues is related to the priorities of juridical development of digital technologies, prospects of legal regulation of digital profiling, experimental and special legal regimes in the sphere of digital innovations, intellectual rights, labor and adjacent relations, blockchain technologies, cryptocurrency, decentralized finance in legal realities, artificial intelligence, robotics, etc.

The research works included in this volume are systematized by the modern trends of digital technologies development in the system of criminal-legal, international-legal and private-legal (civilistic) relations.

The ideas and proposals reflected in this and other volumes are, taken integrally, a key to understanding the intellectual map of meanings, which would be interesting for legal scientists and experts in the sphere of digital technologies, practicing lawyers, representatives of law-making and law-enforcement agencies, state servants and participants of the real economy sector, young researchers – students, graduates and post-graduates, to all those interested in the issues of mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67c51я43

ISBN 978-5-8399-0767-6
ISBN 978-5-8399-0769-0 (Volume 2)

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЙ

Е. Ю. Антонова,
доктор юридических наук, профессор,
Дальневосточный юридический институт (филиал)
Университета прокуратуры Российской Федерации

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Аннотация. В последние годы отмечается активное внедрение различных цифровых технологий в процесс совершения преступлений террористической направленности. Автор поставил перед собой цель выработать рекомендации по противодействию таким преступлениям. Для достижения этой цели были проанализированы различные формы преступной деятельности террористических формирований, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий. Определено, что развитие цифрового пространства и цифровых технологий способствует интенсивности терроризма, а также привело к изменению механизма совершения преступлений террористической направленности. Сделан вывод о том, что для обеспечения эффективности мер по противодействию преступлениям террористической направленности, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий необходимы четкая стратегия и соответствующая нормативная правовая база.

Ключевые слова: цифровые технологии, цифровое пространство, преступления террористической направленности, идеология насилия, пропаганда терроризма, вербовка, финансирование, криминализация, противодействие

THE USE OF DIGITAL TECHNOLOGIES IN THE COMMISSION OF TERRORIST CRIMES: PROBLEMS OF COUNTERACTION

Abstract. In recent years, there has been an active introduction of various digital technologies in the process of committing crimes of a terrorist nature. The author set himself the goal of developing recommendations for countering such crimes. To achieve this goal, various forms of criminal activity of terrorist groups committed in the digital space and (or) using digital technologies were analyzed. It is determined that the development of digital space and digital technologies contributes to the intensity of terrorism and led to a change in the mechanism for committing crimes of a terrorist nature. It is concluded that to ensure the effectiveness of measures to counter terrorist crimes committed in the digital space and (or) using digital technologies, a clear strategy and an appropriate regulatory legal framework are needed.

Keywords: Digital technologies, Digital space, Terrorist crimes, Ideology of violence, Propaganda of terrorism, Recruitment, Financing, Criminalization, Counteraction

Преступления в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий/систем/программ представляют естественную эволюцию преступности, обусловленную научно-техническим прогрессом и новыми разработками, и относятся к числу серьезных проблем современного мира.

Не являются исключением и преступления террористической направленности. Отмечается, что уровень терроризма продолжает расти, как и «технологические достижения, способствующие привлечению внимания и эмоционального воздействия террористов» [16. P. 251]. Исследователями фиксируется прямая связь между цифровым (кибер-) пространством и различными формами социально-политической дестабилизации: антиправительственными демонстрациями, беспорядками и террористическим актами [14. P. 1–34].

Заместитель секретаря Совета безопасности России Ю. Коков справедливо замечает, что наступает эра цифрового терроризма, который по масштабам возможных последствий может быть сопоставим с оружием массового уничтожения. По его данным в Интернете действует около 30 тыс. террористических и экстремистских сайтов [9]. Данные обстоятельства требуют серьезной работы по противодействию преступлениям террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

Формы преступной деятельности террористических формирований, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий. Лица, вовлеченные в террористическую деятельность, активно используют современные цифровые технологии не только в процессе совершения преступлений, но и в повседневной жизни. Такие технологии применяются внутри террористических сообществ/организаций (далее – формирований) в качестве инструмента коммуникации, в том числе в процессе организации террористической деятельности, а также при вербовке членов террористических формирований, распространении идеологии насилия, пропаганды террористической деятельности, призывов к совершению конкретных террористических актов. Террористы стремятся донести такие сообщения, а также продемонстрировать свои противоправные деяния максимально широкой аудитории, поскольку основной их целью является дестабилизация общества, его моральная и политическая нестабильность.

При этом, распространяя через цифровое (кибер-) пространство информацию, не всегда соответствующую действительности (это может быть и дезинформация, слухи, угрозы применения насилия или изображения актов насилия), террористические формирования оказывают воздействие не только на возможных или действительных сторонников террористических воззрений, идеологии насилия (что используется в первую очередь для вербовки новых членов, радикализации, подстрекательства к терроризму, подрыва веры в социальные ценности), но и на прямых или косвенных жертв террористических актов (устрашение населения путем психологического манипулирования, распространения чувств повышенного беспокойства, тревоги, страха или паники среди населения) или на органы власти и международное сообщество в целом (дестабилизация деятельности органов власти или международных организаций либо воздействия на принятие ими решений).

Именно поэтому террористы стремятся адаптировать экстремальные средства коммуникации для привлечения внимания и видимости в глобальной медиасреде. Насилие террористов, в высшей степени опосредованное и зрелищное, порождает превращение атак в медиа-события, которые разворачиваются в гибридной медиасреде и укореняются в доступных возможностях и технологиях [17. P. 1–17].

Для совершения пропагандистских действий террористические формирования задействуют широкий спектр технических средств: веб-сайты, чат-группы и чат-форумы, онлайн-журналы, платформы таких социальных сетей, как Twitter (заблокирован в РФ) и Facebook (экстремистская организация, запрещена в РФ), популярные видео- и файлообменные веб-сайты, например, YouTube. Поисковые системы Интернета упрощают нахождение террористического контента.

На слушаниях в подкомитете по информации и борьбе с терроризмом Комитета Национальной безопасности палаты представителей Правительства США были приведены примеры использования террористами систем искусственного интеллекта (далее – ИИ). Так, один из сторонников превосходства белой расы открыл огонь по двум мечетям в Крайстчерче (Новая Зеландия), убив 51 человека и ранив еще 49. Террорист смог транслировать нападение в прямом эфире на Facebook, потому что ИИ Facebook не счел отснятый материал достаточно ужасным. Затем видео было 300 000 раз успешно загружено на Facebook другими пользователями. Это доказывает, что технологии ИИ, призванные блокировать такие видео, еще не справляются с поставленной задачей. Более того, имеются факты, свидетельствующие о том, что ИИ Facebook снимает видео и продвигает террористический контент, который он должен был удалить [12].

Кроме того, через цифровое (кибер-) пространство происходит вербовка новых членов террористических формирований, их онлайн-обучение; планирование террористических атак.

Отмечается, например, что специализированные террористические сайты работают как онлайн-библиотеки идеологических текстов, платформы для вербовщиков и форумы для обмена информацией. Кроме того, фото- и видеоматериалы, игры (имитирующие террористические атаки и побуждающие пользователей участвовать в ролевой игре, выступая в роли виртуального террориста), учебные пособия и технические инструкции, подготовленные террористическими группами, способствуют радикализации их сторонников [14. P. 1–34]. Пропагандистские материалы могут содержать идеологические или практические руководства, разъяснения, оправдания или рекламу деятельности террористов.

Так, в ходе проверки Шахунской городской прокуратурой Нижегородской области интернет-ресурсов, осуществляемой с использованием программы браузера: «Google Chrome», в поисковом ресурсе «Яндекс», при введении ключевых слов «Expedient Homemade Firearms», отобразился список интернет-сайтов, содержащий ссылки: <данные изъяты>. На указанных интернет-страницах размещены материалы с подробной информацией о способах самостоятельного изготовления оружия, проходит обсуждение этой информации. Доступ к информации свободный для всех пользователей, сайт и интернет-страницы не содержат ограничений к его доступу по кругу лиц, не требуется предварительной регистрации и пароля, ознакомиться

с содержанием данной интернет-страницы и скопировать материалы в электронном варианте может любой интернет-пользователь, ограничения на передачу, копирование и распространение отсутствуют [2].

Как отмечают специалисты, воздействие на компьютерную информацию позволяет преступнику «манипулировать эмоциями и сознанием потерпевшего, вызывая серьезные психофизиологические последствия. Психоэмоциональный эффект сравним по силе с эффектом от событий в реальном мире, в то же время он смоделирован путем изменения компьютерной информации» [6. С. 235]. К таким психологическим приемам и прибегают террористические формирования в процессе вербовки новых членов и пропаганды своей идеологии.

В науке отмечаются феноменальные успехи систем ИИ не только в области цифровых платформ, но и в материальной, непосредственной среде. Это видно на примере внедрения цифровых технологий (современной робототехники) в систему беспилотного управления транспортных средств, что облегчает совершение террористических актов. На практике уже встречаются случаи применения цифровых технологий, в том числе беспилотников, в процессе приготовительной и непосредственной террористической деятельности, в частности для доставки наркотиков, психоактивных веществ и других запрещенных предметов – оружия, взрывчатых веществ, взрывных устройств и пр.

Так, террористические группы все чаще используют беспилотники для наблюдения, взрывов и других действий. Сообщается, что ИГИЛ (запрещенная в РФ организация) начал использовать боевые дроны в Ираке и объявил о создании подразделения «Беспилотные летательные аппараты моджахедов» [15]. Кроме того, ИГИЛ провел несколько бомбардировок с использованием беспилотников, нацеленных как на гражданские, так и на военные цели, и даже предпринимал попытки атаковать беспилотниками глав государств [13]. По мере увеличения производства этих гаджетов и снижения себестоимости эти новшества станут более привлекательными и востребованными для отдельных террористов и групп. Ножи и грузовики все еще могут быть более простыми и дешевыми вариантами, но новые методы атаки также начнут реализовываться [15].

3D-принтеры также могут сделать сложные и дорогие технологии доступными для террористов. Так, напавший на немецкую синагогу в Йом-Кипур в начале октября 2019 г. использовал напечатанные на 3D-принтере компоненты самодельного оружия [15]. В 2020 г. немецкий террорист потратил всего 50 долларов на 3D-печать деталей для оружия, которое использовалось при попытке нападения в Галле [13].

Цифровое (кибер-) пространство используется и в качестве средства для совершения кибератак, призванных нарушить нормальное функционирование компьютерных систем, серверов с помощью компьютерных вирусов, вредоносных и шпионских программ или других средств неправомерного доступа к компьютерной информации. Для этих действий характерны такие черты террористического акта, как стремление путем устрашения населения способствовать дестабилизации деятельности органов власти или международных организаций, воздействовать на принятие ими решений и таким образом достичь политических или иных социальных целей.

Для достижения поставленных целей и эффективной деятельности террористические формирования привлекают значительные материальные ресурсы. Цифровое (кибер-) пространство и новые технологии только способствуют быстрому получению доходов, которые в последующем используются для нужд террористов. Как отмечает руководитель Антитеррористического центра СНГ А. Новиков, «произошла цифровая трансформация механизмов и каналов финансирования терроризма». В качестве источников доходов террористы используют онлайн-казино, прибегают к хищениям денег через подставные интернет-магазины и сайты-двойники, используют фишинговые и фарминг-атаки, несанкционированный доступ к банковским ресурсам и криптовалютным биржам [10]. Кроме того, через цифровое (кибер-) пространство террористические формирования обращаются с прямыми просьбами о пожертвованиях. Для этого используются веб-сайты, чат-группы, массовые рассылки сообщений с просьбами о пожертвованиях.

Так, Северо-Кавказский окружной военный суд вынес обвинительный приговор в отношении Ш., который опубликовал в Интернете призыв к сбору денежных средств на нужды ИГИЛ. Полученные деньги он перевел на счет террористической группировки [3]. В другом случае следствием и судом установлено, что М. перечислил через платежный терминал 7000 руб. на счет электронного кошелька, который использовался для сбора денежных средств с целью финансовой помощи членам группировки «Хайят Тахрир аш-Шам», являющейся структурным подразделением запрещенной террористической организации «Джебхат ан-Нусра» [5].

Веб-сайты используются и в качестве интернет-магазинов, предлагающих книги, аудио-, видеозаписи и иные материалы с соответствующим содержанием.

Преимущества использования цифрового пространства и (или) цифровых технологий обусловлены, во-первых, скоростью передачи данных и распространения информации (дезинформации), а также обработки большого массива информации, позволяющей, например, оперативно отыскивать сторонников, вербовать новых членов террористических формирований и т. д.; во-вторых, охватом неопределенно широкой аудитории и расширением географии распространения деструктивной идеологии насилия в условиях относительной анонимности; в-третьих, сложностью контролирования содержательной части распространяемой информации; в-четвертых, упрощением координации действий членов террористических формирований.

Кроме того, к очевидным преимуществам цифровых технологий относят возможность их использования на любых, в том числе представляющих опасность территориях (зоны военных конфликтов); физическую безопасность субъектов, их применяющих (при использовании опасных предметов – химических, отравляющих или взрывчатых веществ и др.) и сложность их обнаружения [1. С. 35].

Перечисленные и иные факторы во многих случаях увеличивают и степень общественной опасности совершаемых деяний, что должно быть отражено и в нормах уголовного закона.

Особо привлекательной для террористических формирований в этом плане является несовершеннолетняя аудитория, поскольку она не имеет необходимого жизненного опыта, устойчивых положительных ориентаций и является активным пользователем цифрового (кибер-) пространства. К тому же, как отмечается в на-

учной литературе, «подростки подвержены формированию установок на агрессивное поведение». Наиболее действенными в отношении них являются технологии разжигания агрессии посредством экстремистских лозунгов, политизации социально-экономических проблем, романтизации образов «отрицательных героев», навязывания идей, пропагандирующих насилие как социальную норму и погружения их в деструктивные интернет-сообщества [11. С. 127–130]. Для вербовки несовершеннолетних применяются популярные музыкальные видеоролики, компьютерные игры, мультипликационные фильмы, рассказы, поощряющие и прославляющие действия террористов, миссии террористов-смертников и др.

Так, трое 15-летних подростков с октября 2019 г. по июнь 2020 г. «путем общения в одной из социальных сетей и мессенджерах, придерживаясь идей анархизма… объединились в группу для последующего совместного осуществления террористической деятельности на территории города Канска». Распределив между собой роли, подростки самостоятельно проходили обучение путем чтения запрещенной, признанной решением суда экстремистской литературы и просмотра видеофильмов по изготовлению взрывчатых веществ и взрывных устройств в целях осуществления террористической деятельности. Они самостоятельно изготавливали взрывчатые вещества и взрывные устройства и отрабатывали их применение на практике в заброшенном доме, на пустырях и стройках с целью подготовки к совершению террористического акта путем подрыва здания полиции или УФСБ. В материалах дела фигурировали скриншоты переписок в социальных сетях, в которых фигуранты дела обсуждали, где и как приобрести компоненты взрывчатки. Кроме того, школьники намеревались «для наглядности» построить в игре Minecraft здание ФСБ и взорвать его [8].

Все вышесказанное подтверждается и специалистами в области противодействия терроризму. Так, директор Контртеррористического управления ООН В. Воронков отмечает, что террористы активно пользуются различными технологическими достижениями. Используя социальные сети, зашифрованные сообщения («даркнет»), они распространяют свою человеконенавистническую идеологию, собирают и переводят средства, радикализируют молодежь и вербуют новых сторонников, координируют теракты. Причем они задействуют алгоритмы социальных сетей так, чтобы как можно быстрее и шире распространять свой контент. Есть данные о попытках террористического подполья использовать лекарственные препараты для создания биологического оружия. Для доставки химических, биологических или радиологических материалов, террористы могут применять беспилотники, в том числе автоматические [4].

Для противодействия преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий требуется выработка эффективных механизмов уголовно-правового воздействия, которые позволят своевременно реагировать на террористические угрозы в цифровой среде. Новые задачи стоят и перед правоохранительными органами, которые должны оперативно выявлять источник угрозы и блокировать его.

Несмотря на то, что в российское уголовное законодательство вносятся изменения: нормы дополняются квалифицирующим (особо квалифицирующим)

признаком «совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет», видоизменяются и появляются новые нормы о преступлениях против компьютерной информации, пока нельзя констатировать наличие должной, эффективной системы мер уголовно-правового воздействия на лиц, совершающих рассматриваемые деяния в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий. Анализ норм уголовного закона показывает, что к настоящему времени законодатель усилил лишь ответственность за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма (ст. 2052 УК РФ), в случае их совершения в цифровом (кибер-) пространстве (ч. 2). Во всех остальных нормах о преступлениях террористической направленности соответствующий квалифицирующий (особо квалифицирующий) признак отсутствует. Вместе с тем практика показывает, что цифровое (кибер-) пространство используется не только для распространения пропагандистской информации в террористических целях, но и для содействия террористической деятельности, включая вербовку новых членов террористических формирований, финансирование, обучение исполнителей, подстрекательство к совершению террористических актов и др.

Проведенный анализ различных форм преступной деятельности террористических формирований, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, позволяет констатировать:

1) развитие цифрового (кибер-) пространства (социальных сетей, электронных СМИ и других интернет-ресурсов), увеличение числа пользователей таким пространством и цифровыми технологиями/системами/программами способствует расширению идеологии насилия за счет активной пропагандистской деятельности террористических формирований, и как результат интенсивности терроризма;

2) использование цифровых технологий террористическими формированиями, по сути, ведет к изменению механизма совершения преступлений террористической направленности – от стадии приготовления до оконченного преступления и сокрытия его следов.

Данные обстоятельства должны быть учтены и при выработке конструктивных, эффективных мер по противодействию преступлениям террористической направленности. Современные цифровые технологии необходимо активнее использовать в процессе выявления, раскрытия и расследования преступлений террористической направленности, особенно когда таковые совершаются в цифровом (кибер-) пространстве, а также с использованием IT-технологий. Важным аспектом в этой связи является возможность использования ИИ оперативно-разыскными подразделениями (например, система распознавания лиц, идентификация личности, номеров транспортных средств, мониторинг социальных сетей и т. д.).

Цифровое (кибер-) пространство может эффективно быть использовано для проведения оперативно-разведывательных действий, сбора информации, извлекаемой из сообщений на веб-сайтах, в чатах и других цифровых ресурсах, что будет способствовать своевременному предотвращению и пресечению террористических актов, сбору доказательственной базы для привлечения лиц к уголовной ответственности.

Еще одной контрмерой является создание веб-сайтов, чат-групп, чат-форумов и других интернет-платформ для ведения конструктивных онлайн-дискуссий, демонстрации контртеррористических и иных воспитательно-просветительских материалов, опирающихся на конкретные факты, изложения альтернативных насильственным методов решения политических и иных социальных проблем.

Для эффективного выявления, раскрытия и расследования преступлений террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, сотрудники правоохранительных органов должны обладать не только правовыми, но и специальными техническими знаниями по механизму данных преступлений. Они должны знать современные цифровые (компьютерные, информационно-коммуникационные) технологии/системы/программы, порядок их работы.

Таким образом, для обеспечения эффективности мер по противодействию преступлениям террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, необходима четкая стратегия и соответствующая нормативная правовая база, которые должны быть нацелены на:

1) криминализацию (изменение интенсивности пенализации) общественно опасных деяний (в том числе террористической направленности), совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий. Для этого необходима ревизия уголовного закона и иных нормативных правовых актов в сфере цифровых технологий в целях выявления пробелов правовой защиты объектов от террористических угроз и определения потребности усиления ответственности в конкретных случаях. Допускаем, что совершение преступлений в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий не во всех случаях может увеличивать степень общественной опасности запрещенных деяний. В этой связи на современном этапе считаем достаточным дополнить ст. 63 УК частью 12 и изложить ее в следующей редакции «12. Судья (суд), назначающий наказание, в зависимости от характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного может признать отягчающим обстоятельством совершение преступления с использованием цифровых и информационно-телекоммуникационных технологий»;

2) усиление сил и средств на воспитательно-просветительскую деятельность, в том числе в цифровом (кибер-) пространстве, направленную на пропаганду «мирного сосуществования всех народов независимо от расы, национальности, языка, происхождения в противовес негативному информационно-идеологическому воздействию на личность извне, в том числе пропаганды идеологии терроризма» [7. С. 207];

3) обучение сотрудников правоохранительных органов, выявляющих и расследующих преступления, в том числе террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий;

4) расширение полномочий сотрудников правоохранительных органов для обеспечения четкого и эффективного контроля цифрового контента;

5) выработку соглашений по международному сотрудничеству в области противодействия преступлениям, в том числе террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

Список литературы

1. Антонова Е. Ю. Технологии искусственного интеллекта – субъект преступления или орудие/средство совершения преступления? // Юридический вестник Кубанского государственного университета. 2022. № 1 (14). С. 31–39. DOI: https://doi.org/10.31429/20785836-14-1-31-39

2. Архив Шахунского районного суда Нижегородской области. Решение № 2А-214/2021 от 22 марта 2021 г. Дело № 2А-214/2021 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/AAQ1OEJsQbb9/ (дата обращения: 27.07.2022).

3. В Дагестане суд приговорил собиравшего средства для ИГ мужчину к 17 годам // РБК. URL: https://www.rbc.ru/rbcfreenews/5d44544c9a7947190c12566e (дата обращения: 26.07.2022).

4. В Минске обсуждают возможности новых технологий и искусственного интеллекта в борьбе с терроризмом // Организация Объединенных Наций. URL: https://news.un.org/ru/story/2019/09/1362292 (дата обращения: 30.07.2021).

5. В Российской Федерации вынесен приговор за финансирование терроризма // Eurasian Group. URL: https://eurasiangroup.org/ru/sentence-for-terrorist-financing-in-russian-federation34 (дата обращения: 26.07.2022).

6. Дремлюга Р. И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение: монография. Москва: Юрлитинформ. 328 с.

7. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология: учебное пособие. Москва: Академия управления МВД России, 2021. 244 с.

8. Подростка из Канска приговорили к 5 годам колонии за подготовку теракта // Деловой Петербург. URL: https://www.dp.ru/a/2022/02/10/Podrostka_iz_Kanska_prigo (дата обращения: 27.07.2022).

9. СБ РФ: цифровой терроризм может быть сопоставим с оружием массового уничтожения // ТАСС. URL: https://tass.ru/politika/14658343/amp (дата обращения: 27.07.2022).

10. Террористы все активнее используют IT-технологии, заявили в АТЦ СНГ // РИА Новости. URL: https://ria.ru/amp/20200218/1564913906.html (дата обращения: 26.07.2022).

11. Щетинина Е. В. Проблемы развития культуры насилия в интернет-пространстве // Инновационное развитие профессионального образования. 2018. № 2 (18). С. 127–130.

12. Artificial Intelligence and Counterterrorism: Possibilities and Limitations // Hearing Before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security House of Representatives One Hundred Sixteenth Congress. First Session. June 25, 2019. Serial № 116–28. Washington: U. S. Government Publishing Office, 2020. 48 p.

13. Gavin J. Trends in Terrorism [2022] // Vision of Humanity. URL: https://www.visionofhumanity.org/trends-in-terrorism/ (дата обращения: 26.07.2022).

14. Khokhlov N., Korotayev A. Internet, Political Regime and Terrorism: A Quantitative Analysis // Cross-Cultural Research. 2022. Vol. 0 (0). Pp. 1–34. DOI: 10.1177/10693971221085343

15. Noor E. Sharing space: Tech and terrorism // Observer Research Foundation. URL: https://www.orfonline.org/expert-speak/sharing-space-tech-terrorism-60862/ (дата обращения: 25.07.2022).

16. Orehek E., Vazeou-Nieuwenhuis A. Understanding the Terrorist Threat: Policy Implications of a Motivational Account of Terrorism // Policy Insights from the Behavioral and Brain Sciences. 2014. Vol. 1 (1). Pp. 248–255.

17. Uusitalo N., Valaskivi K., Sumiala J. Epistemic modes in news production: How journalists manage ways of knowing in hybrid media events involving terrorist violence // Journalism. 2021. 16 May. Pp. 1–17. DOI: 10.1177/14648849211015601

Т. П. Афонченко,
кандидат юридических наук, доцент,
Белорусский торгово-экономический
университет потребительской кооперации

К ПРОБЛЕМЕ СОВЕРШЕНСТВОВАНИЯ УГОЛОВНО-ПРАВОВЫХ НОРМ В КОНТЕКСТЕ ВЫЗОВОВ ИНФОРМАТИЗАЦИИ

Аннотация. Целью представленного исследования является анализ проблем криминализации отдельных видов составов преступлений (хищений), совершаемых посредством использования цифровых технологий, в том числе в глобальной сети Интернет, в контексте обеспечения прав на безопасность каждого индивида. На основе изучения действующих нормативных актов формулируются предложения по совершенствованию национального уголовного законодательства Республики Беларусь посредством усиления уголовно-правовой репрессии в отношении виновных, использующих цифровую среду и цифровые технологии в качестве места и способа совершения преступления.

Ключевые слова: цифровые технологии, информационно-коммуникативная среда, преступное посягательство, уголовно-правовое воздействие, объект уголовно-правовой охраны, способ совершения преступления, мошенничество

TO THE PROBLEM OF IMPROVEMENT OF CRIMINAL LEGAL NORMS IN THE CONTEXT OF INFORMATIZATION CHALLENGES

Abstract. The purpose of the presented study is to analyze the problems of criminalization of certain types of offenses (theft) committed through the use of digital technologies, including on the global Internet, in the context of ensuring the rights to security of each individual. Based on the study of the current regulations, proposals are formulated to improve the national criminal legislation of the Republic of Belarus by strengthening criminal law repression against the perpetrators who use the digital environment and digital technologies as a place and method of committing a crime.

Keywords: Digital technologies, Information and communication environment, Criminal infringement, Criminal legal impact, Object of criminal legal protection, Method of committing a crime, Fraud

Введение. Информационно-коммуникативные технологии и цифровая среда в настоящее время выступают системообразующим элементом функционирования социума, оказывающим разнообразное существенное влияние на динамику и качество развития политической, экономической, производственной и социально-культурной деятельности в обществе. Интенсивность развития цифровизации, активный запрос на использование виртуальных технологий в повседневной действительности, темпы роста, опережающие уровень развития иных сфер, не всегда позволяют своевременно обеспечить надлежащую правовую платформу, а следовательно, адекватный уровень защиты гарантируемых прав и свобод индивида. Не являются исключением в рассматриваемом смысле и общественные отношения, выступающие объектом уголовно-правовой охраны.

Основная часть. Конституция Республики Беларусь, определяя элементы правового статуса личности, формулирует концептуальные подходы на предмет приоритетов защиты тех или иных охраняемых благ [3]. Информация либо право на безопасную информационную среду как самостоятельная конституционно-правовая категория в настоящее время не выступает. Иными словами, Основной Закон белорусского государства не формулирует специфического права на защиту и безопасную коммуникацию в виртуальном пространстве. В то же время, положениями Концепции национальной безопасности Республики Беларусь информационная безопасность определена как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [4].

Уголовный кодекс Республики Беларусь в действующей редакции (далее по тексту – УК) закрепляя перечень объектов уголовно-правовой охраны закрепляет в ст. 2, информационно-коммуникативная среду и ее составляющие в качестве самостоятельной группы однородных общественных отношений, нуждающихся в защите с помощью механизма уголовно-правового воздействия, не называет [6]. Действительно, в настоящее время степень проникновения цифровых технологий в различные охраняемые законом сферы настолько велика и развивается со столь бурной скоростью, что четко маркировать границы общественных отношений, связанных с информационно-коммуникативной деятельностью, в том числе для целей обеспечения, собственно, их безопасности и безопасности вовлеченных в них субъектов, – физических и юридических лиц, – представляется весьма затруднительным, если вообще возможным. В то же время, нельзя отрицать очевидный факт того, что преступные посягательства, совершаемые в сегменте информационной сети Интернет (в том числе в рамках функционирования социальных сетей и социальных мессенджеров, организации торговых площадок в дистанционной форме, игрового и иного развлекательного контента), а также с помощью или исключительно посредством компьютерных и иных информационных технологий, достаточно велика. Как справедливо отмечает К. А. Амиянц, «возможные криминальные угрозы и пути их уголовно-правового предупреждения» требуют детального осмысления [1. С. 150] и, на наш взгляд, адекватного отражения в нормах уголовного закона.

Колоссальная степень концентрации пользователей, свободный и комфортный доступ к разнообразному контенту (от узкопрофессионального до различных форм

досугового), отсутствие у подавляющего большинства пользователей базовых знаний и навыков об информационной этике и безопасности, а также об элементарных механизмах защиты своих материальных и нематериальных интересов в Сети делает виртуальное пространство все более привлекательном с точки зрения его использования в качестве платформы противоправной деятельности. Формы последней могут быть также самыми разнообразными, как связанными с посягательствами на честь и достоинство личности, охраняемую законом тайну, так и затрагивающие имущественные интересы пользователей. Информация, являясь стратегическим фактором развития современного общества, получая воплощение и объективацию различными способами, является целью преступных посягательств как сама по себе (результаты авторского права и объекты интеллектуальной собственности, ноу-хау и коммерческая, государственная тайна), так и в качестве средства получения доступа к иным благам материального и нематериального характера.

Официальные статистические сведения, обобщаемые и обнародуемые, демонстрируют беспрецедентный всплеск преступлений рассматриваемой группы в Республике Беларусь. Так, по сравнению с 2017 г. в 2021 г. только зарегистрированное количество хищений с использованием компьютерной техники и преступлений в сфере информационной безопасности выросло с 3111 случаев практически в пять раз и составило 15 503 случая [1. С. 24; 4. С. 152], что делает рассматриваемый сегмент преступности одним из самых динамично растущих. Представляется возможным предположить, что подобная ситуация находится в резонансе с общемировыми тенденциями. В связи с указанным обращает на себя внимание феномен мошенничеств, совершаемых в глобальной информационной сети, а также с использованием различных социальных мессенджеров, когда потерпевшие сообщают о себе значимую информацию, используемую в дальнейшем злоумышленниками для хищения денежных средств, аккумулируемых на банковских счетах, либо передают денежные средства самостоятельно, добровольно совершая денежные переводы в пользу непосредственно виновных либо третьих лиц. Потерпевшие могут полагать, что собеседник имеет право на получение информации либо денежных средств в силу якобы занимаемой должности, выполняемой трудовой функции (злоумышленник представляется сотрудником банка, правоохранительной структуры) либо в связи со сложившимися личными взаимоотношениями (злоумышленник создает иллюзию дружеского участия, влюбленности, демонстрирует альтруизм). Иными словами, обман (злоупотребление доверием) используются как самостоятельный способ совершения преступления либо как способ облегчения совершения кражи. Несмотря на широкий общественный резонанс названных преступлений, системную профилактическую работу банковских организаций и органов, осуществляющих уголовное преследование (личные беседы с держателями карт, информационная рассылка в популярных мессенджерах и размещение наглядных и доступных для восприятия материалов с предупреждениями о формах и методах совершаемых преступлений, публикации в печатных и иных средствах массовой информации) даже случаи, когда одни и те же потерпевшие становятся жертвами интернет-мошенников, по-прежнему отнюдь не единичны. Представляется, что в формате дистанционного общения срабатывает так называемый эффект «случайного попутчика», когда

у потерпевшего формируется по отношению к собеседнику неоправданно высокий уровень доверия, позволяющий эффективно реализовать преступный замысел.

Повышенная степень уязвимости потенциального потерпевшего с точки зрения актуальной уголовной репрессии белорусским законодателем в настоящее время в должной степени не учтена, хотя определенные законодательные решения, направленные на противодействие преступных посягательств, связанных с развитием информационных технологий, в УК реализованы. Так, носители компьютерной информации сами по себе могут вступать предметом преступления, в частности, в таких составах преступлений, как «Несанкционированный доступ к компьютерной информации» (ст. 349), «Уничтожение, блокирование или модификация компьютерной информации» (ст. 350), «Неправомерное завладение компьютерной информацией» (ст. 352), «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств» (ст. 354), «Нарушение правил эксплуатации компьютерной системы или сети» (ст. 355), расположенных в самостоятельном разделе XII УК «Преступления против компьютерной безопасности» [6]. В определенных ситуациях уголовный закон рассматривает элементы цифровой среды и их программное обеспечение как способ совершения преступления (ст. 212 УК «Хищение имущества путем модификации компьютерной информации»). Сеть Интернет в ряде случаев оценивается как место совершения преступления (ст. 188 УК «Клевета» криминализирует в качестве альтернативного деяния распространение наказуемых сведений «… в информации, размещенной в глобальной компьютерной сети Интернет, иной сети электросвязи общего пользования или выделенной сети электросвязи») [6]. Подобным образом решается вопрос о месте совершения преступления (размещения информации) в ст. 1302 УК «Отрицание геноцида белорусского народа», ст. 3431 УК «Изготовление и распространение порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего».

Статьи 205 УК «Кража» и 209 УК «Мошенничество», рассматривая в качестве отягчающих ответственность признаков, влияющих на квалификацию (квалифицирующий и особо квалифицирующие составы преступления), совершение преступления повторно, группой лиц, с проникновением в жилище, в крупном размере, а также организованной группой либо в особо крупном размере, повышенную степень опасности использования информационно-коммуникативных технологий при совершении хищения путем обмана или злоупотребления доверием потерпевшего либо путем использования последних для совершения тайного хищения имущества, не предусматривает.

Кроме того, по смыслу национальных гражданско-правовых норм о возмещении морального вреда причинение имущественного ущерба, в том числе в рамках хищения, не является основанием для компенсации нравственных страданий. В силу того, что при противоправном использовании информации, полученной в Сети, виновное лицо посягает также на принадлежащие потерпевшем нематериальные блага, предлагаем включить рассматриваемые ситуации в перечень оснований, кода моральный вред подлежит компенсации наряд с причиненным имущественным ущербом.

Заключение. В дискурсе интенсификации использования информационных технологий как в части сфер их проникновения, так и с точки зрения количества пользователей, становится вполне очевидным и закономерным возникновение и совершенствование инновационных общественных отношений, реализуемых в цифровом пространстве, что актуализирует обеспечение их охраны, в том числе с помощью уголовно-правовых средств. Представляется, что с учетом актуальной криминологической ситуации целесообразно усиление уголовной репрессии путем дополнения отдельных составов преступлений, предусматривающих ответственность за хищения, признаком использования элементов цифровой среды. Таким образом, предлагаем: 1) дополнить ч. 2 ст. 205 и ч. 2 ст. 209 УК РФ признаком использования информационно-коммуникативных технологий; 2) рассмотреть вопрос о расширении перечня оснований возмещения морального вреда в случаях, если имущественный вред причинен преступным посягательством с использованием информации, полученной посредством информационно-коммуникативных технологий.

Список литературы

1. Амиянц К. А. Искусственный интеллект и уголовное право: постановка проблемы // Уголовное право в системе межотраслевых связей: проблемы теории и правоприменения: материалы XIII Российского конгресса уголовного права, состоявшегося 26–27 мая 2022 г. Москва: Юрлитинформ, 2022. С. 150–154.

2. Беларусь в цифрах: статистический справочник / Национальный статистический комитет Республики Беларусь. Минск: Республиканское унитарное предприятие «Информационно-вычислительный центр Национального статистического комитета Республики Беларусь», 2022. 69 с.

3. Конституция Республики Беларусь от 15 марта 1994 г.: принята на Респуб. реф. 24 нояб. 1996 г., 17 окт. 2004 г., 27 фев. 2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2022. URL: https://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/konstitutsiya-respubliki-belarus.

4. Концепция национальной безопасности Республики Беларусь: утверждена Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2022. URL: https://etalonline.by/document/?regnum=p31000575

5. Статистический ежегодник Республики Беларусь, 2021 г.: стат. сб. / Национальный статистический комитет Респ. Беларусь. Минск, 2021. 407 с.

6. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информации Республики Беларусь. Минск, 2022. URL: https://etalonline.by/document/?regnum=HK9900275

Д. Д. Берсей,
кандидат юридических наук, доцент,
Северо-Кавказский федеральный университет

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ОБЗОР СОВРЕМЕННЫХ ЗАРУБЕЖНЫХ НАУЧНЫХ ИССЛЕДОВАНИЙ

Аннотация. В статье проведен обзор зарубежных исследований в области социальной инженерии. В обзоре представлены современные данные зарубежных научных исследований о сущности социальной инженерии и вопросов противодействия ей. Проанализированы публикации авторов, в работах которых рассмотрены различные проблемы в рамках темы исследования, а также проанализированы публикации, в которых разбираются различные проблемы в рамках исследуемой темы. В статье проанализирована эволюция развития подходов к изучению социальной инженерии.

Ключевые слова: социальная инженерия, кибербезопасность, кибератака, конфиденциальная информация, информация, контрмеры, персональные данные, прайминг

SOCIAL ENGINEERING: A REVIEW OF MODERN FOREIGN SCIENTIFIC RESEARCH

Abstract. The article provides a review of foreign research in the framework of social engineering. The review presents up-to-date data from foreign scientific research on social engineering and issues of countering it. The publications of authors whose works considered various problems within the framework of the research topic were analyzed, as well as the publications of authors whose works considered various problems within the framework of the research topic were analyzed. The article analyzes the evolution of the development of approaches to the study of social engineering.

Keywords: Social engineering, Cybersecurity, Cyberattack, Confidential information, Information, Countermeasures, Personal data, Priming

Введение. При написании данной статьи был выявлен и проанализирован достаточно широкий спектр проблем: это и эволюция подходов к социальной инженерии в рамках кибербезопасности, шаблоны и сценарии атак социальной инженерии, проблемы развития контрмер против атак социальной инженерии, расширенные атаки социальной инженерии, особенности вредоносного программного обеспечения для социальной инженерии. Также в исследуемых работах сравниваются алгоритмы атак и защиты для онлайн социальных сетей, изучаются особенности работы хакеров в рамках социальной инженерии, рассматривают направления снижения рисков и ущерба от действий социальной инженерии с учетом человеческого фактора, а также выявляют необходимость этики в исследованиях социальной инженерии. Соответственно, широта взглядов зарубежных исследователей позволяет заключить, что рассматриваемая в статье проблема противодействия социальной инженерии имеет высокую актуальность, теоретическую и практическую значимость.

Этот метод применяется с целью выполнения финансовых операций, излома, кражи данных, например, клиентских баз, персональных данных и другой несанкционированного доступа к информации. Социальная инженерия помогает конкурентам осуществлять разведку, выявлять слабые стороны организации, переманивать сотрудников.

Вопросы социального инжиниринга в отечественных научных кругах появился во времена резкого увеличения доступности информационных ресурсов, телекоммуникационных сетей и терминалов пользователей.

Принципы воздействия на человека с помощью методов социальной инженерии приведены в работах [1]. Общие вопросы утечки данных рассмотрены в [2, 3], непосредственно социального инжиниринга – в работах [4, 5]. Проблема предоставления доступа к служебной информации рассмотрена в [6].

Социальная инженерия представляет собой область знаний, к которой, в связи с развитием цифровых технологий, обращаются в последнее время как отечественные, так и зарубежные специалисты. При этом объектом изучения исследователей становятся различные аспекты указанной категории – от технических и технологических до социологических, психологических и правовых. В этой связи интересным представляется анализ публикаций зарубежных авторов в рамках заявленной темы исследования.

Joseph M. Hatfield рассматривает особенности эволюции подходов к социальной инженерии в рамках кибербезопасности. В работе автора предлагается история концепции социальной инженерии в кибербезопасности и утверждается, что, хотя первоначально данный термин был предметом изучения политологии и только позже получил распространение в области кибербезопасности, он представляет собой приложение одних и тех же фундаментальных идей: эпистемической асимметрии, технократического доминирования и телеологической замены. Далее в статье утверждается, что использование этого термина в обеих областях остается концептуально и семантически взаимосвязанным. Более того, незнание этой взаимосвязи продолжает ограничивать нашу способность выявлять и отражать атаки социальной инженерии в киберпространстве.

Автор рассматривает историю развития термина с предпосылок, возникших в XIX в. в трудах экономистов Джона Грея и Торстейна Веблена. Анализ научных статей показывает, что эта концепция получала распространение на протяжении всего периода с начала до середины XX в. в рамках социальных наук и за их пределами. Затем в статье прослеживается трансформация концепции в кибербезопасность на протяжении 1960–1980-х гг., для чего исследуются как научные публикации, так и мемуарные отчеты, включая интервью с активными участниками хакерского сообщества того времени. Наконец, исследователь раскрывает концептуальный массив современных коннотаций через анализ 134 определений этого термина, найденных в академических статьях, написанных о кибербезопасности с 1990 по 2017 г. [1].

Исследователи Francois Mouton, Louise Leenen, H. S. Venter исследуют примеры, шаблоны и сценарии атак социальной инженерии. Авторы приходят к выводу, что информационная безопасность – это быстро развивающаяся дисциплина. Несмотря на то, что эффективность мер безопасности по защите конфиденциальной информа-

ции растет, люди по-прежнему подвержены манипуляциям, и поэтому человеческий элемент остается слабым звеном.

Атака социальной инженерии нацелена на эту слабость, и специалисты в этой области используют различные методы манипулирования для получения конфиденциальной информации. Область социальной инженерии все еще находится на ранних стадиях своего развития в том, что касается формальных определений, рамок атак и шаблонов атак.

В рассматриваемой статье предлагаются детальные шаблоны атак социальной инженерии, полученные на основе реальных примеров социальной инженерии. Современные документированные примеры атак социальной инженерии не включают все этапы и фазы атаки. Предлагаемые шаблоны атак социальной инженерии призваны облегчить проблему ограниченной информации по атакам социальной инженерии путем сопоставления реальных примеров с рамками атак социальной инженерии.

Сопоставление нескольких подобных примеров из реального мира с моделью атаки социальной инженерии позволяет установить детальный поток атаки, абстрагируясь от субъектов и объектов. Это сопоставление затем используется для предложения обобщенных шаблонов атак социальной инженерии, которые являются репрезентативными для реальных примеров, но все же достаточно общими, чтобы охватить несколько различных реальных примеров. Предлагаемые шаблоны атак социальной инженерии охватывают все три типа коммуникации, а именно двунаправленную коммуникацию, однонаправленную коммуникацию и косвенную коммуникацию.

Авторы считают, что для проведения сравнительных исследований различных моделей социальной инженерии, процессов и структур необходимо иметь формализованный набор сценариев атаки социальной инженерии, которые полностью детализированы на каждом этапе и этапе процесса. Шаблоны атак социальной инженерии преобразуются в сценарии атак путем заполнения шаблона как субъектами, так и объектами из реальных примеров, сохраняя при этом детальный поток атаки, как это предусмотрено в шаблоне.

Кроме того, эта статья иллюстрирует, как сценарии атаки социальной инженерии применяются для проверки модели обнаружения атаки социальной инженерии. Указанные шаблоны и сценарии могут быть использованы другими исследователями для расширения, использования для сравнительных показателей, создания дополнительных примеров или оценки моделей для полноты. Кроме того, предлагаемые шаблоны атак в области социальной инженерии также могут быть использованы для разработки информационных материалов в области социальной инженерии.

Richard Power, Dario Forte рассматривают проблему низких темпов развития контрмер против атак социальной инженерии. Они указывают, что социальная инженерия звучит как материал шпионских фильмов, но это очень реальная жизнь, как показывают некоторые недавние громкие дела. Социальная инженерия работает очень эффективно, представляя собой мощную психологическую технику.

Скандал с HP, в котором участвовали следователи, выдающие себя за членов совета директоров, сотрудников и журналистов, чтобы получить телефонные за-

писи, показывает, насколько далеко пойдут решительные социальные инженеры. Однако некоторые сотрудники HP зашли совсем далеко, и директорам пришлось подать заявление в Комиссию по ценным бумагам и биржам США (SEC), признав нарушения компании.

Социальная инженерия – это угроза, которая изощренно эволюционировала в последнее десятилетие, однако развитие контрмер в данной области значительно отстает. Единственная реальная контрмера заключается в необходимости повышения осведомленности персонала в вопросах безопасности.

Существует два типа социальной инженерии: технологический и человеческий обман. Социальные инженеры часто заявляют, что они настоящие сотрудники, и просят прислать им по электронной почте конфиденциальную информацию по действительному адресу, а также внешнему. Все сотрудники, особенно те, кто обладает конфиденциальной информацией, включая руководителей, персонал отдела кадров и личных администраторов, должны знать, как распознать мошенника за милю. А сотрудников нужно научить сохранять спокойствие и не раскрывать свои подозрения мошеннику. Эксперты по безопасности Ричард Пауэр и Дарио Форте анализируют тактику специалистов по социальной инженерии, которую персонал должен остерегаться.

Социальная инженерия, практика обмана людей в обмен на конфиденциальную информацию, представляет собой угрозу кибербезопасности, которая развивалась в совершенстве и расширялась в масштабах на протяжении десятилетия. К сожалению, в большинстве организаций контрмеры против социальной инженерии не получают должного развития [2].

В статье «Возможности автоматического анализа поверхностных атак сетевой социальной инженерии» авторы указывают, что процесс социальной инженерии нацелен на людей, а не на ИТ-инфраструктуру. Злоумышленники используют обманные уловки для создания убедительных поведенческих «крючков», которые, в свою очередь, преследуют цель получить от оппонента конфиденциальную информацию или заставить его взаимодействовать с вредоносным ПО. Создание таких «крючков» базируется на личной информации, которую люди публикуют о себе в интернете, особенно в социальных сетях. Несмотря на то, что существующие исследования отмечают сложности подобной методики социальной инженерии, связанные с получением данных из открытых источников, последняя активно применяет с этой целью ресурсоемкий ручной анализ или интерактивные методы сбора информации. Однако ручной анализ большого объема информации не всегда продуктивен, а интерактивные методы могут вызвать ряд вопросов у исследуемого субъекта. По этой причине специалисты социальной инженерии постоянно находятся в поиске альтернатив [3].

Авторы в своем исследовании демонстрируют, что ключевая информация, относящаяся к атакам социальной инженерии на организации, может быть пассивно собрана в крупном масштабе в автоматическом режиме. В центре работы находятся две ключевые проблемы. С одной стороны, исследователи демонстрируют, как можно автоматически идентифицировать сотрудников организации, используя только ту информацию, которая находится в свободном доступе. С другой стороны,

в статье рассмотрено, каким образом после идентификации профили сотрудников могут быть связаны между несколькими онлайновыми социальными сетями для сбора дополнительной информации, относящейся к успешным атакам социальной инженерии. После исследователи демонстрируют авторский подход в рамках организации атаки методами социальной инженерии реальных ключевых инфраструктурных организаций. В результате проведенного анализа в статье предложен набор контрмер, включая автоматизированный сканер уязвимостей социальной инженерии, который организации могут использовать для анализа своей подверженности потенциальным атакам социальной инженерии [4].

M. Junger, L. Montoya, F.-J. Overink считают, что предупреждения не эффективны для предотвращения атак социальной инженерии [5]. Они отмечают, что люди склонны доверять друг другу и легко раскрывать личную информацию. Это делает их уязвимыми для атак социальной инженерии. В работе была изучена эффективность двух мероприятий, направленных на защиту пользователей от атак социальной инженерии, а именно прайминг с помощью сигналов для повышения осведомленности об опасностях кибератак социальной инженерии и предупреждение о раскрытии личной информации. Была изучена выборка посетителей торгового района среднего города в Нидерландах. Раскрытие информации измерялось путем запроса у испытуемых их адреса электронной почты, 9 цифр из их 18-значного номера банковского счета, а также те, кто ранее делал покупки в интернете, опрашивались на предмет того, что они приобрели и в каком интернет-магазине. Были обнаружены относительно высокие показатели раскрытия информации: 79,1 % испытуемых заполнили свой электронный адрес, а 43,5 % предоставили информацию о банковских счетах. Среди интернет-покупателей 89,8 % испытуемых указали тип продукта(ов), который они приобрели, и 91,4 % указали название интернет-магазина, в котором они сделали эти покупки. Многомерный анализ показал, что ни прайминг вопросов, ни предупреждение не влияют на степень раскрытия информации. Были обнаружены признаки неблагоприятного воздействия предупреждения. Последствия сделанных выводов, как считают авторы, могут быть самыми неблагоприятными для опрошенных [5].

Ryan Heartfield, George Loukas исследуют проблему обнаружения атак семантической социальной инженерии с помощью самого слабого звена. В качестве которого выступает человек. Представление о том, что человек-пользователь является самым слабым звеном в информационной безопасности, подвергалось критике в последние годы. Авторы показывают, что человек-пользователь действительно может быть самым сильным звеном для обнаружения атак, связанных с обманом, таких как маскировка приложений, Wi-Fi evil twin и другие виды семантической социальной инженерии. В этом направлении мы разработали фреймворк human-as-a-security-sensor, получивший практическую реализацию в виде Cogni-Sense, прототипа приложения Microsoft Windows, предназначенного для того, чтобы позволить и поощрять пользователей активно обнаруживать и сообщать о семантических атаках социальной инженерии против них.

Экспериментальная оценка с участием 26 пользователей различных профилей, использующих Cogni-Sense на своих персональных компьютерах в течение 45 дней,

показала, что человеческие сенсоры могут стабильно превосходить технические системы безопасности. Используя подход, основанный на машинном обучении, мы также показываем, что надежность каждого отчета и, следовательно, производительность каждого человеческого датчика могут быть предсказаны осмысленным и практическим образом. В организации, использующей реализацию датчика безопасности человека, например Cogni-Sense, считается, что атака была обнаружена, если хотя бы один пользователь сообщил об этом.

По оценкам авторов, небольшая организация, состоящая только из 26 участников эксперимента, продемонстрировала бы коэффициент пропущенного обнаружения ниже 10 %, по сравнению с 81 %, если бы использовались только технические системы безопасности. Полученные результаты убедительно указывают на необходимость активного вовлечения пользователя не только в профилактику с помощью кибергигиены и ориентированного на пользователя дизайна безопасности, но и в активное обнаружение киберугроз и отчетность о них [6].

Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl исследуют в своей работе расширенные атаки социальной инженерии. Они считают, что социальная инженерия превратилась в серьезную угрозу для виртуальных сообществ и является эффективным средством атаки на информационные системы. Услуги, используемые сегодняшними работниками умственного труда, подготавливают почву для сложных атак социальной инженерии. Растущая тенденция к политике BYOD (bring your own device) и использовании инструментов онлайн-коммуникации и совместной работе в частной и деловой среде усугубляют эту проблему. В глобально действующих компаниях команды расположены отдаленно друг от друга, и снижение личного взаимодействия сочетается с большим количеством инструментов, используемых для общения (электронная почта, IM, Skype, Dropbox, LinkedIn, Lync и др.), что формирует благоприятную почву для создания новых векторов атаки для атак социальной инженерии. Недавние атаки на такие компании, как The New York Times и RSA, показали, что целенаправленные атаки на копье-фишинг являются эффективным эволюционным шагом в данной области. Они становятся опасным оружием, которое часто используется продвинутыми специалистами в области социальной инженерии. Авторы приводят в своем исследовании таксономию хорошо известных атак социальной инженерии, а также всесторонний обзор передовых атак социальной инженерии на работника умственного труда [7].

Sherly Abraham, InduShobha Chengalur-Smith проводят обзор вредоносного ПО для социальной инженерии, анализируя его тенденции, тактику и последствия [8]. Они считают, что социальная инженерия продолжает оставаться растущим вектором атаки для распространения вредоносных программ. Для этой статьи авторы собрали данные об инцидентах с вредоносными программами и выделили распространенность и долговечность вредоносных программ социальной инженерии.

Также исследователи разработали структуру, которая показывает шаги, которые выполняет вредоносная программа социальной инженерии, чтобы быть успешным. Чтобы объяснить его распространенность и постоянство, в статье представлены некоторые общие пути, по которым происходят такие атаки. Вектор атаки представляет собой комбинацию психологических и технических уловок, которая включает

в себя заманивание пользователя компьютера для выполнения вредоносного ПО и борьбу с любыми существующими техническими контрмерами.

В работе также рассмотрены некоторые распространенные психологические уловки и технические контрмеры, используемые вредоносными программами социальной инженерии. Исследовано направление развития методов, используемых поставщиками таких вредоносных программ, чтобы обойти существующие контрмеры.

Результаты анализа позволяют нам подчеркнуть как важность планирования организациями комплексной программы информационной безопасности, так и общую социальную ответственность, необходимую для борьбы с вредоносными программами социальной инженерии [8].

Поведение человека включает культуру, потребности и стремления как отдельных людей, так и групп. В отношении ИТ существует множество сообществ или групп людей, каждое из которых имеет собственные потребности, стремления и поведение. Например, для людей, использующих информационные системы, характерны потребности, связанные с удобством пользования и эргономикой, а также с доступностью и производительностью. Люди, чьи должностные обязанности изменяются из-за использования ИТ, могут обладать потребностями, связанными с коммуникацией, обучением и ободрением. У людей, участвующих в создании и эксплуатации ИТ-ресурсов, могут быть потребности, связанные с условиями работы и развитием компетенций.

Majd Latah проводит исследование в области обнаружения вредоносных социальных ботов [8]. Он считает, что социальные боты представляют собой новое поколение ботов, которые используют онлайновые социальные сети (OSNs) в качестве каналов командования и управления (C&C).

Вредоносные социальные боты использовались в качестве инструментов для запуска крупномасштабных спам-кампаний, продвижения акций с низкой капитализацией, манипулирования цифровым влиянием пользователей и проведения политического астротурфинга. Последние исследования в этой области либо сосредоточены только на общих проблемах безопасности, связанных с социальными сетями, либо на грубой классификации для поддержки подходов к обнаружению.

Опрос, проведенный в статье, призван обеспечить всесторонний анализ с точки зрения социальных сетей. С этой целью автор сначала классифицирует атаки социальных ботов на разных стадиях, а затем предоставляет обзор различных типов социальных ботов.

Далее автор предлагает уточненную таксономию, которая показывает, как различные методы в рамках категории связаны или отличаются друг от друга, а затем подробно обсуждаются сильные и слабые стороны каждого метода. После этого рассматриваются существующие наборы данных и обобщаются результаты эмпирических исследований, на основе чего выделяются ограничения существующих подходов к обнаружению и предлагаются будущие направления дальнейшего совершенствования. Автор считает, что его исследование должно помочь администраторам OSN и исследователям понять разрушительный потенциал вредоносных социальных ботов и улучшить текущие защитные стратегии [9].

Mingzhen Mo, Irwin King, Kwong-Sak Leung проводят эмпирические сравнения алгоритмов атак и защиты для он-лайн социальных сетей. Онлайн-социальные сети, такие как Facebook, являются популярными сайтами социальных сетей, на которых сотни миллионов пользователей заводят друзей и взаимодействуют с людьми. Существует большое количество личной информации на этих сетевых сайтах, и их безопасность скорее беспокоит как пользователей, так и исследователей, потому что ценная частная информация принесет большую прибыль некоторым людям или группам.

В реальном мире прибыль мотивирует людей и группы получать личные данные незаконно, и многие атаки запускаются в социальных сетях. При столкновении с различными атаками исследователи предлагают различные защитные стратегии, направленные на снижение негативного эффекта атак. Однако практическая эффективность защит неизвестна, когда они борются с реальными атаками. Кроме того, мы также мало понимаем, насколько сильными будут атаки, когда они сталкиваются с защитой. Поэтому в данной статье предлагается схема сравнения Attack-Protect-Attack (APA) для изучения производительности и смещения различных алгоритмов атаки и защитных стратегий для онлайновых социальных сетей. Таким образом, результаты сравнения являются ценными и значимыми для дальнейшей защиты частной информации.

Авторы предлагают применить несколько атакующих и защитных подходов к реальному набору данных из Facebook, а затем оцениваем их по точности алгоритмов атаки. Следуя схеме сравнения, экспериментальным путем можно убедиться, что эффективность защитных стратегий не является удовлетворительной в сложном и практическом случае [10].

Brian Anderson, Barbara Anderson в своем исследовании «Социальная инженерия и USB объединяются для жестокой атаки» исследуют совокупность знаний, широко известных как социальная инженерия, представленную с точки зрения тестирования на проникновение. Они изучают эволюционирующие области, приводят практические примеры, строят портативную платформу проникновения и обсуждают, как бороться с этими умными конфронтациями.

Авторы приходят к мысли, что хотя социальная инженерия и философия проникновения существуют уже несколько тысячелетий, каждая из них постоянно развивается и адаптируется к информационным технологиям.

Социальная инженерия вообще может рассматриваться как предмет более широкого спектра социальных наук. В то время как определение социальных наук обычно относится к крупномасштабным приложениям, концепция влияния на отношения, популярные убеждения, поведение и ресурсы довольно хорошо переносится в технологический сектор.

Благодаря своей портативности и простоте использования, неудивительно, что флеш-накопители стали самым популярным носителем информации на сегодняшний день. Распространение этих накопителей можно в значительной степени объяснить халявой продавцов, раздаваемой на занятиях, семинарах или любом мероприятии, предоставляющем пробные версии продукта, маркетинг или документацию. Эти устройства теперь можно найти в широком диапазоне декоративных

или скрывающих обложек, которые включают в себя чернильные ручки, наручные часы и всевозможные новинки. Несмотря на простой способ хранения информации, флеш-накопитель повышает возможность развертывания тайных операций.

Абсолютная безопасность на самом деле никогда не может быть достигнута; обеспечение безопасности – это непрерывный процесс, требующий постоянного внимания и регулирования. Для поддержания эффективного положения в области безопасности все элементы, связанные с окружающей средой, должны постепенно укрепляться по мере поступления новых угроз и развития предприятий. Продолжать использовать программное обеспечение в качестве единственного механизма защиты нецелесообразно [11].

Особенности работы хакеров в рамках социальной инженерии рассмотрены в работе Johnny Long, Scott Pinzon, Jack Wiles, Kevin D. Mitnick. Они отмечают, что социальная инженерия – самое важное оружие в арсенале нетехнического хакера. Нетехнический хакер – это в равной степени оппортунист, актер и мошенник. Эксперты по безопасности сводят все это и многое другое в термине «социальный инженер». Хакер экспериментирует с частью технологии, чтобы увидеть, может ли он получить от нее полезные результаты, которые ее создатель никогда не предполагал. Социальный инженер делает то же самое с человеческими отношениями.

Социальная инженерия не полагается на неисправное высокотехнологичное оборудование, чтобы организовать атаку. Скорее всего, он использует искусную атаку на психику противника. В большинстве случаев это можно сделать с помощью буфера обмена и дешевой визитной карточки. Таким образом, помимо того, что это легко, социальная инженерия может быть грязно-дешевой. Одна из лучших защит против социальной инженерии – это осознанность. Каждый сотрудник должен быть обучен тому, как легко можно использовать социальную инженерию, какую большую угрозу она представляет, если ее не обнаружить, и некоторым простым контрмерам [12].

Jack Wiles, Terry Gudaitis, Jennifer Jabbusch, Russ Rogers, Sean Lowther исследуют различные темы социальной инженерии, от понимания умов хакеров и жертв до методов защиты личной, бытовой и деловой информации от кражи и уничтожения.

Социальная инженерия стала самым ценным и эффективным инструментом низкотехнологичных хакеров, которые продолжают использовать искусство аферы, чтобы получить доступ к интеллектуальной собственности и, если это необходимо, к зданиям, в которых находится эта собственность. Авторы приводят несколько примеров, иллюстрирующих, как социальные инженерные атаки происходят в домах и на предприятиях, а также возможные меры по их предотвращению.

Сегодня каждая область, связанная с безопасностью, включает в себя управление рисками, связанными с сохранением безопасности и защищенности. Большинство инструментов социальной инженерии приходят из дворовых распродаж, благотворительных магазинов, блошиных рынков, ломбардов и интернета. Это касается шляп, пиджаков с фирменными логотипами, ремней для инструментов, инструментов, подслушивающих устройств, портфелей, шпионских программ и замков, которые могут быть достаточно эффективно использованы для социальной инженерии.

Общая скрытность угроз, связанных с социальной инженерией, позволяет социальным инженерам очень легко застать кого-либо врасплох. В этой главе

также описывается ряд полезных контрмер по управлению рисками в отношении социальной инженерии [13].

Tayouri D. рассматривает направления снижения рисков и ущерба от действий социальной инженерии с учетом человеческого фактора.

Люди – это социальные существа, и цифровая эра не изменила этого, но она изменила способ нашего общения. Используя социальные сети, пользователи имеют мгновенный доступ к миллионам людей, расширяя свое взаимодействие с ними. Но у социальных сетей есть риски для безопасности. Они также используются преступниками для мошенничества, сбора бизнес-аналитики, кражи конфиденциальной информации и т. д.

В своей работе автор демонстрирует риски кибербезопасности и меры их смягчения, уделяя особое внимание человеческому фактору и социальным сетям. Формальной политики для руководства тем, как сотрудники могут использовать сайты социальных сетей, недостаточно, и необходимы дополнительные условия: образование, начиная с начальной школы, интерактивное и адаптируемое обучение и инновационные технологические средства. Чтобы усилить человеческий фактор необходимо приложить усилия в образовании, начиная уже с первого класса, в том возрасте, когда дети подвергаются воздействию интернета.

Необходимо использовать необычные подходы к обучению кибербезопасности, такие как интерактивные видеоигры. Но необходимо также приложить больше усилий к технологическим средствам, помогающим людям совершать меньше ошибок и избегать попадания в кибер-ловушки.

Настройки конфиденциальности могут ограничить доступ к информации пользователя. Инструменты мониторинга сайтов социальных сетей могут помочь организациям отслеживать вредоносные действия и угрозы в отношении них. Технология может помочь проверить надежность человека, предлагающего дружбу.

Социальные сети также можно использовать для выявления инсайдерской угрозы организации, анализируя контент социальных сетей. Сочетание образования и обучения с лучшими в своем роде технологиями может снизить риски и ущерб социальной инженерии [14].

Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter исследуют необходимость этики в исследованиях социальной инженерии. Они отмечают, что социальная инженерия глубоко укоренилась как в области компьютерных наук, так и в области социальной психологии. Знания требуются в обеих этих дисциплинах для выполнения исследований, основанных на социальной инженерии.

При проведении исследований в области социальной инженерии необходимо учитывать ряд этических соображений и требований, с тем чтобы не допустить причинения вреда тем, кто участвует в таких исследованиях. Эти проблемы и требования еще не были формализованы, и большинство исследователей не знают об этических проблемах, связанных с исследованиями в области социальной инженерии.

Исследователь выявляет ряд проблем, связанных с социальной инженерией в области общественных коммуникаций, тестированием на проникновение и исследованиями в области социальной инженерии. В работе также обсуждаются выявленные проблемы в отношении трех различных нормативных этических подходов

(этика добродетели, утилитаризм и деонтология) и приводятся соответствующие им этические перспективы, а также практические примеры того, где эти формализованные этические проблемы для исследований социальной инженерии могут быть полезны [15].

Waldo Rocha Flores, Mathias Ekstedt в своей статье рассматривают возможности противостояния социальной инженерии через трансформационное лидерство, культуру информационной безопасности и осведомленность. В работе проведено эмпирическое исследование того, как организационные и индивидуальные факторы дополняют друг друга в формировании намерения сотрудников противостоять социальной инженерии.

Исследование проводилось с использованием смешанных методов исследования, в ходе которых были собраны качественные данные как для создания исследовательской модели исследования, так и для разработки инструмента обследования, который был распространен среди 4296 сотрудников организаций из различных организаций, расположенных в Швеции. Результаты показали, что отношение к сопротивлению социальной инженерии имеет самую сильную прямую связь с намерением сопротивляться социальной инженерии, в то время как самоэффективность, так и нормативные убеждения демонстрируют слабую связь с намерением сопротивляться социальной инженерии.

Кроме того, авторами было отмечено, что трансформационное лидерство тесно связано как с воспринимаемой культурой информационной безопасности, так и с осознанием информационной безопасности. Два медиативных теста продемонстрировали, что отношение и нормативные убеждения частично опосредуют влияние культуры информационной безопасности на намерение сотрудников противостоять социальной инженерии. Это говорит о том, что как отношение, так и нормативные убеждения играют важную роль в регулировании отношений между культурой информационной безопасности и намерением противостоять социальной инженерии.

Третий опосредующий тест показал, что культура информационной безопасности полностью объясняет влияние трансформационного лидерства на отношение сотрудников к сопротивлению социальной инженерии. Также в работе приводится обсуждение результатов и практических последствий проведенных исследований [16].

Таким образом, проведенное исследование позволяет сделать вывод о том, что направления исследований зарубежных специалистов в рамках изучения различных аспектов социальной инженерии представлены в достаточно широком спектре. Авторы рассматривают такие проблемы, как особенности эволюции подходов к социальной инженерии в рамках кибербезопасности, примеры, шаблоны и сценарии атак социальной инженерии, низкие темпы развития контрмер против атак социальной инженерии, расширенные атаки социальной инженерии, особенности вредоносного ПО для социальной инженерии. Также авторы сравнивают алгоритмы атак и защиты для онлайн социальных сетей, исследуют совокупность знаний, широко известных как социальная инженерия, представленную с точки зрения тестирования на проникновение, изучают особенности работы хакеров в рамках социальной инженерии, рассматривают направления снижения рисков и ущерба от действий социальной инженерии с учетом человеческого фактора, а также выявляют необходимость этики в исследованиях социальной инженерии.

Если анализировать даты написания рассмотренных работ, можно увидеть, что с основном они относятся к последнему десятилетию. Однако исследование, посвященное контрмерам в социальной инженерии датировано 2006 годом, что позволяет говорить об обращении к данной проблеме на заре развития социальной инженерии и понимании специалистами всей остроты существующей проблемы уже почти 15 лет назад.

Соответственно, можно заключить, что с каждым годом проблема социально-инженерных атак и необходимости защиты от них обостряется, что предопределяет обращению к ней специалистов различных областей: информационной безопасности и защиты информации, психологии и социологии, политологии и экономики, информационного и административного права, уголовного права и криминологии.

Заключение. Цель данной статьи состояла в объяснении определения социальной инженерии, основанное на связанных теориях многих смежных дисциплин, таких как психология, социология, информационные технологии, маркетинг и бихевиоризм. Благодаря этой работе мы надеемся помочь исследователям, практикам, юристам и другим лицам, принимающим решения, получить более полное представление о социальной инженерии и, следовательно, открыть новые направления сотрудничества для ее выявления и контроля.

Увеличение использования электронных средств связи (электронная почта, IM, Skype и т. д.) В корпоративных средах созданы новые векторы атак для социальных инженеров. Миллиарды людей в настоящее время используют электронное оборудование в своей повседневной работе, что означает миллиарды потенциальных жертв атак социальной инженерии (SE). Человек считается самым слабым звеном в цепи кибербезопасности, и нарушение этой защиты в настоящее время является наиболее доступным путем для злонамеренных внутренних и внешних пользователей. Хотя несколько методов защиты уже были предложены и применены, ни один из них не фокусируется на атаках SE на основе чата, в то же время автоматизация на местах все еще отсутствует. Социальная инженерия представляет собой сложное явление, требующее междисциплинарных исследований, сочетающих технологии, психологию и лингвистику. Злоумышленники рассматривают черты человеческой личности как уязвимые места и используют язык как свое оружие для обмана, убеждения и, наконец, манипулирования жертвами, как они хотят, поведение человека (human behavior): взаимодействие людей и других элементов системы.

Область информационной безопасности является динамично развивающейся сферой. Даже несмотря на это эффективность мер безопасности для защиты конфиденциальной информации растет, люди остаются восприимчивыми к манипуляциям и, таким образом, человеческий фактор остается слабым звеном. Социоинженерные атаки используют в достижении своих цели эту слабость, используя различные методы манипуляции, чтобы получить конфиденциальную информацию. Сфера социальной инженерии все еще находится на ранних стадиях в отношении формальных определений, рамок атак и шаблонов атак. Предлагаются подробные шаблоны социоинженерных атак, которые вытекают из реальных примеров социальной инженерии. Современные документированные примеры социоинженерных атак не включают в себя все этапы и фазы атаки.

Предлагаемые шаблоны социальной инженерии атаки пытаются облегчить проблему ограниченного документированной литературы по социотехники посредством отображения реальных примеров в рамках социальной инженерии атаки. Картирование несколько подобных реальных примеров в рамках социальной инженерии атаки позволяет установить точный поток атаки в то время, как абстрагируются субъекты и объекты. Это отображение затем используется, чтобы предложить обобщенные шаблоны атак социальной инженерии, которые являются репрезентативными реальных примеров, в то время еще достаточно общим, чтобы охватить несколько различных реальных примеров. Предлагаемые шаблоны социальной инженерии атаки охватывают все три типа связи, а именно двунаправленной связи, однонаправленной связи и косвенной связи. Для проведения сравнительных исследований различных методов социальной инженерии моделей, процессов и структур, необходимо иметь формализованный набор сценариев социальной инженерии атаки, которые полностью описаны в каждой фазе и стадии процесса. Шаблоны социальной инженерии атаки преобразуются в сценарии социальной инженерии атаки путем заполнения шаблона с обоими субъектами и объектами из реальных примеров в то время, как все еще сохраняя точный поток атаки, как это предусмотрено в шаблоне. Кроме того, этот документ показывает, как сценарии социальной инженерии атаки применяются для проверки модели обнаружения атак социальной инженерии. Эти шаблоны и сценарии могут быть использованы другими исследователями либо расширить, использовать для сравнительных мер, создать дополнительные примеры или оценки моделей для полноты картины. Кроме того, предлагаемые шаблоны социальной инженерии атаки, также могут быть использованы для разработки социальной инженерии материалов осведомленности.

Список литературы

1. Joseph M. Hatfield Social engineering in cybersecurity: The evolution of a concept // Computers & Security. 2018. Vol. 73. March. Pp. 102–113.

2. Richard W. Power, Dario V. Forte Social engineering: attacks have evolved, but countermeasures have not // Computer Fraud & Security. 2006. Vol. 10. October. Pp. 17–20.

3. Francois Mouton, Louise Leenen, H. S. Venter Social engineering attack examples, templates and scenarios // Computers & Security. 2016. Vol. 59. June. Pp. 186–209.

4. Matthew Edwards, Robert Larson, Benjamin Green, Awais Rashid, Alistair Baron. Panning for gold: Automatically analysing online social engineering attack surfaces // Computers & Security. 2018. Vol. 69. August. Pp. 18–34.

5. Junger M., Montoya L., Overink F. -J. Warnings are not effective for preventing social engineering attacks // Computers in Human Behavior. 2018. Vol. 66. January. Pp. 75–87.

6. Ryan Heartfield, George Loukas Human-as-a-security-sensor for harvesting threat intelligence // Computers & Security. 2018. Vol. 76. July. Pp. 101–127.

7. Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl Advanced social engineering attacks // Journal of Information Security and Applications. 2015. Vol. 22. June. Pp. 113–122.

8. Sherly Abraham, InduShobha Chengalur-Smith An overview of social engineering malware: Trends, tactics, and implications // Technology in Society. 2010 Vol. 32. Iss. 3. August. Pp. 183–196.

9. Majd Latah Detection of malicious social bots: A survey and a refined taxonomy // Expert Systems with Applications. 2020. Vol. 1511. August. Article 113383.

10. Mingzhen Mo, Irwin King, Kwong-Sak Leung Empirical Comparisons of Attack and Protection Algorithms for Online Social Networks // Procedia Computer Science. 2011. Vol. 5. Pp. 705–712.

11. Brian Anderson, Barbara Anderson CHAPTER 7 – Social Engineering and USB Come Together for a Brutal Attack / Seven Deadliest USB Attacks. 2010. Pp. 177–217.

12. Johnny Long, Scott Pinzon, Jack Wiles, Kevin D. Mitnick No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing // No Tech Hacking. 2008. Pp. 101–119.

13. Jack Wiles, Terry Gudaitis, Jennifer Jabbusch, Russ Rogers, Sean Lowther Social engineering: The ultimate low tech hacking threat / Low Tech Hacking. 2012. Pp. 1–29.

14 Joseph M. Hatfield The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages // Computers & Security. 2019. Vol. 83. June. Pp. 354–366.

15. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2019. Vol. 55. November. Pp. 114–127.

16. Waldo Rocha Flores, Mathias Ekstedt Shaping intention to resist social engineering through transformational leadership, information security culture and awareness // Computers & Security. 2016. Vol. 59. June. Pp. 26–44.

17. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2015. Vol. 55. November. Pp. 114–127.

16. Mouton, F.a b, Leenen, L.a, Venter, H.S.b Social engineering attack examples, templates and scenarios // Computers and Security. 2016. Vol. 59. Pp. 186–209.

И. И. Бикеев,
доктор юридических наук, профессор,
Казанский инновационный университет имени В. Г. Тимирясова

НЕКОТОРЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРОТИВОДЕЙСТВИИ КОРРУПЦИИ

Аннотация. Целью исследования является изучение современного опыта использования цифровых технологий в противодействии коррупции в Российской Федерации и внесение на этой основе предложений по совершенствованию данного вида деятельности. Анализируется значение цифровых технологий для разных направлений противодействия коррупции. Рассмотрен опыт как субъектов Российской Федерации (на примере Республики Татарстан), так и федеральных органов власти.

Ключевые слова: цифровые технологии, противодействие коррупции, государственная информационная система, «Народный контроль», «Посейдон», закупки для государственных и муниципальных нужд, конфликт интересов

SOME ISSUES OF THE USE OF DIGITAL TECHNOLOGIES IN THE ANTI–CORRUPTION

Abstract. The purpose of the work is to study the modern experience of using digital technologies in the anti-corruption in the Russian Federation and to make proposals on this basis to improve this type of activity. The importance of digital technologies for different areas of anti-corruption is analyzed. Both the experience of the subjects of the Russian Federation (on the example of the Republic of Tatarstan) and the experience of federal authorities are considered.

Keywords: Digital technologies, Anti-corruption, State information system, "People's Control", "Poseidon", Procurement for state and municipal needs, Conflict of interests

Введение. Коррупция как особая часть преступности является исключительно сложным негативным социальным явлением. Ее сложность относится к самым разным вопросам: причинам, формам проявления, последствиям [11, 13, 14] и т. д. Кроме того, названное явление быстро трансформирующееся, мимикрирующее под изменения внешней среды. А значит, и механизм противодействия ей тоже должен быть динамичным и перманентно совершенствуемым [9, 15]. Для такого противодействия используются различные инструменты и средства, а также постоянно осуществляется поиск новых инструментов и средств соответственно [5].

В последние годы во всех странах мира, включая и Российскую Федерацию, все большее распространение получают цифровые технологии, значение которых сложно переоценить в силу их многоаспектности. Причем данное утверждение относится ко всем направлениям противодействия коррупции, указанным в ст. 1 Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции». Так, цифровые технологии важны и как инструмент предупреждения коррупционных правонарушений, обеспечивающий прозрачность и подконтрольность деятельности официальных лиц и тем самым воздерживающий их от совершения ненадлежащих деяний [6], и как средство борьбы с коррупцией, позволяющее выявлять соответствующие правонарушения, а также успешно их расследовать. И, наконец, как инструмент, позволяющий минимизировать и даже ликвидировать последствия коррупционных правонарушений. Например, выявить и найти незаконно полученные нарушителем выгоды.

Вместе с тем цифровые технологии в сфере противодействия коррупции еще не применяются столь широко, как они того заслуживают. И данная проблема нуждается в постоянных действиях по ее решению.

Основная часть. Цифровые технологии в противодействии коррупции используются на разных уровнях и в различных формах. Например, в Республике Татарстан успешно функционирует государственная информационная система «Народный контроль», в которую каждый зарегистрированный в ней гражданин вправе направить обращение о какой-либо проблеме [1]. Такая проблема может относиться к любой сфере: жилищно-коммунальное хозяйство, благоустройство, качество работы государственных и муниципальных органов власти и др. Отдельно фиксируются сообщения о предполагаемых фактах коррупции. Уполномоченные органы изучают обращения и в обязательном порядке дают на них ответ гражданам. В случае если факты, указанные в обращении, подтверждаются, то идет соответствующее реагирование: на-

рушение устраняется, то или иное мероприятие включается в план работы, виновное лицо привлекается в установленном порядке к юридической ответственности и т. д.

Серьезный антикоррупционный эффект имеет и реализуемая в Республике Татарстан Система электронного документооборота, которая позволяет детально отслеживать этапы прохождения того или иного документа и выявлять узкие места его движения.

На федеральном уровне для противодействия коррупции также активно используются цифровые технологии. Так, Специальное программное обеспечение «Справки БК» позволяет единообразно заполнять сведения о доходах, расходах и обязательствах имущественного характера соответствующих категорий лиц.

Имеются и другие перспективные разработки. Например, Указом Президента Российской Федерации от 25 апреля 2022 г. № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации» определены органы власти, ответственные за обеспечение работы указанной системы, а также утверждено положение о ней [10]. Она будет способна обрабатывать огромные массивы разнообразной информации, осуществляя поиск в базах данных различных органов власти, внутренних документах организаций, общедоступных источниках, в том числе социальных сетях. И в результате обеспечивать анализ и проверку соблюдения соответствующими лицами антикоррупционных ограничений, требований и запретов. По мнению К. В. Кабанова, «…российская власть получила суперсистему, способную вычислять взяточников… Искусственный интеллект должен искать все пересечения и совпадения» [2]. Полагаем, что у данной системы большое будущее.

Заключение. На основании изложенного выше представляется, что совершенствование использования цифровых технологий в противодействии коррупции следует осуществлять по следующим приоритетным направлениям:

1. Установление наличия конфликта интересов при осуществлении закупок для государственных и муниципальных нужд [7, 12], что необходимо для обеспечения экономической безопасности государства и муниципальных образований. На наш взгляд, ресурс улучшения ситуации в данной сфере колоссальный.

2. Установление наличия конфликта интересов при решении кадровых вопросов [8], что будет противодействовать созданию организованных групп коррупционной направленности [4]. К сожалению, на наш взгляд, этому направлению уделяется внимания меньше, чем оно заслуживает. Между тем продвижение по службе ставленников групповых интересов (своего рода «амбассадоров коррупции») чрезвычайно опасно.

3. Реализация таких «отложенных» во времени инструментов противодействия коррупции, как антикоррупционное просвещение, антикоррупционное образование и антикоррупционная пропаганда, что позволит резко повысить их эффективность [3].

Список литературы

1. Бадрутдинов М. С. Реализация антикоррупционной политики Республики Татарстан в 2020 году // Антикоррупционный бюллетень: Реализация антикоррупционной политики в Республике Татарстан. Вып. 10 / под ред. М. С. Бадрутдинова. Казань: Бриг, 2021. С. 8–24.

2. Беляков Е., Адамович О. На взяточников натравят искусственный интеллект: Как будет работать антикоррупционная система «Посейдон» // Комсомольская правда. 2022. 25 апреля. URL: https://www.kp.ru/daily/27383/4578300/ (дата обращения: 19.09.2022).

3. Бикеев И. И., Кабанов П. А. Антикоррупционное просвещение: вопросы теории и практики: монография. Серия: Противодействие коррупции. В 3 т. Т. 3. Казань: Изд-во «Познание» Казанского инновационного университета, 2019. 240 с.

4. Глазкова Л. В. Взаимодействие систем организованной преступности и коррупции // Актуальные проблемы российского права. 2019. № 7 (104). URL: https://cyberleninka.ru/article/n/vzaimodeystvie-sistem-organizovannoy-prestupnosti-i-korruptsii (дата обращения: 19.09.2022).

5. Горшенков Г. Н. Коррупция как криминологическая категория // Russian Journal of Economics and Law. 2021. № 15 (3). С. 540–555. URL: https://doi.org/10.21202/2782–2923.2021.3.540–555

6. Латыпова Э. Ю., Кирпичников Д. В. Цифровые средства минимизации коррупционных рисков // Диалектика противодействия коррупции: материалы X Всероссийской научнопрактической конференции с международным участием, 27 ноября 2020 г. Казань: Изд-во «Познание» Казанского инновационного университета, 2021. С. 52–57.

7. Погулич О. В. Конфликт интересов как фактор коррупции в сфере государственной службы // Вестник Забайкальского государственного университета. 2015. № 7 (122). URL: https://cyberleninka.ru/article/n/konflikt-interesov-kak-faktor-korruptsii-v-sfere-gosudarstvennoy-sluzhby (дата обращения: 19.09.2022).

8. Сергеева Г. Правовое обеспечение урегулирования конфликта интересов // Государственная служба. 2010. № 2. URL: https://cyberleninka.ru/article/n/pravovoe-obespechenie-uregulirovaniya-konflikta-interesov (дата обращения: 19.09.2022).

9. Скоробогатов А. В., Скоробогатова А. И., Краснов А. В. Дискурс коррупции в российском обществе // Russian Journal of Economics and Law. – 2021. – № 15(4). – С. 751–764.

10. О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации: Указ Президента Российской Федерации от 25 апреля 2022 г. № 232 // Собрание законодательства Российской Федерации. – 2022. – № 18. – Ст. 3053.

11. Озина А. М., Каришина И. Е. Коррупция в органах государственной власти: проблемы, последствия, меры противодействия // Kant. 2020. № 3 (36). URL: https://cyberleninka.ru/article/n/korruptsiya-v-organah-gosudarstvennoy-vlasti-problemy-posledstviya-mery-protivodeystviya (дата обращения: 19.09.2022).

12. Шмелева М. В. Предотвращение коррупции и других злоупотреблений в сфере государственных закупок // Российское право: образование, практика, наука. 2018. № 1 (103). URL: https://cyberleninka.ru/article/n/predotvraschenie-korruptsii-i-drugih-zloupotrebleniy-v-sfere-gosudarstvennyh-zakupok (дата обращения: 19.09.2022).

13. Aidt T. S. Rent seeking and the economics of corruption // Const. Polit. Econ. 2016. № 27. Pp. 142–157. URL: https://doi.org/10.1007/s10602–016–9215–9 (дата обращения: 19.09.2022).

14. Danon M. Contemporary economic research of corruption // Contemporary Legal and Economic Issues. 2011. Т. 3. С. 252–268.

15. Jeppesen K. K. The role of auditing in the fight against corruption // The British Accounting Review. 2019. Т. 51, № 5. С. 100798.

Д. В. Боев,
ассистент кафедры уголовного права и процесса,
Белгородский государственный национальный
исследовательский университет

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация. В статье исследован опыт европейских стран по применению искусственного интеллекта в уголовном судопроизводстве. Описана проблема применения искусственного интеллекта в соответствии с правами и свободами человека. Рассмотрена перспектива применения искусственного интеллекта в уголовном судопроизводстве при условии соблюдения прав и свобод человека, равенства всех перед Законом, защите персональных данных. В целях избежания нежелательных последствий при использовании искусственного интеллекта в уголовном судопроизводстве предлагаю учитывать опыт европейских стран.

Ключевые слова: право, цифровые технологии, уголовное судопроизводство, Европейская этическая хартия, права и свободы человека, искусственный интеллект, судебные акты

USING ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEEDINGS

Abstract. The article examines the experience of European countries in the use of artificial intelligence in criminal proceedings. The problem of using artificial intelligence in accordance with human rights and freedoms is described. The prospect of using artificial intelligence in criminal proceedings is considered, provided that human rights and freedoms are respected, everyone is equal before the Law, and personal data protection is protected. In order to avoid undesirable consequences when using artificial intelligence in criminal proceedings, I suggest taking into account the experience of European countries.

Keywords: Law, Digital technologies, Criminal proceedings, European Ethical Charter, Human rights and freedoms, Artificial intelligence, Judicial acts

В настоящее время широко применяется искусственный интеллект в юриспруденции, создаются автоматизированные рабочие места (АРМ) юристов, адвокатов, следователей, судей [3. С. 6]. Применение искусственного интеллекта в юриспруденции значительно облегчает и ускоряет процесс судопроизводства.

В мировом сообществе искусственный интеллект не вызывает возражений, потому что является неотъемлемой частью технического прогресса, а продукты цифровых технологий значительно ускоряют процесс исполнения повторяющихся операций.

Для использования в уголовном процессе возможностей искусственного интеллекта требуется правовое регулирование, так как в действующем законодательстве России не дано определение «искусственный интеллект» [2. С. 79].

В научном сообществе пока не сформулировано единого мнения по определению искусственного интеллекта.

Технологии искусственного интеллекта в странах Европы в уголовном судопроизводстве стали применяться не так давно. Применение данных технологий в Европе обусловлено ростом уголовных преступлений, совершенных беженцами. В уголовном судопроизводстве стали применяться системы, обеспечивающие электронный доступ к информации по уголовным делам. Продукты искусственного интеллекта используются европейскими полицейскими при выявлении и раскрытии преступлений. Например, система Connect, применяется полицейскими при оценке финансовых операций. Указанная система позволила сократить обработку баз данных с нескольких месяцев до нескольких минут при большом объеме данных [7]. В раскрытии преступлений связанных с сексуальной эксплуатацией детей, используется международная база данных ICSE DB [8].

Применение искусственного интеллекта вызывает беспокойство европейских юристов, так как работа европейских органов полиции становиться все более не контролируемой, за счет применения цифровых технологий.

Это, в свою очередь, приводит в некоторых случаях к серьезным нарушениям основных прав граждан и затрудняет их доступ к правосудию [1].

В 2018 г. Еврокомиссией принята Этическая хартия использования искусственного интеллекта в судебных системах [5. С. 15–21]. Этическая хартия содержит основные принципы, которые должны выполняться при применении искусственного интеллекта в уголовном судопроизводстве. Основным положением вышеупомянутого документьа является соблюдение основных прав и свобод человека.

Европейский опыт показывает, что применение цифровых технологий открывает возможности для обеспечения прозрачности, предсказуемости и стандартизации правовой системы, но и несет в себе определенные последствия связанные с рисками ограниченности и предвзятости аргументации программного обеспечения [6].

Остро стоит проблема ответственности разработчиков искусственного интеллекта, когда причиняется вред, возникает правонарушение, созданное тем или иным программным продуктом. Так, в 2018 г. во время испытания перед беспилотным автомобилем компании Uber, в темноте на дорогу выскочила велосипедистка, которая погибла во время столкновения с беспилотным автомобилем Volvo XC 90. Водитель беспилотного автомобиля не заметил погибшую женщину до момента столкновения. К ответственности за случившееся правонарушение были привлечены разработчики программного обеспечения машины [9].

Водитель Tesla Model S уснул за рулем, машиной управлял автопилот. Полицейские канадской провинции Альберта, обвинили водителя в опасном вождении, выразившемся в превышении скорости автомобилем в июле 2020 г. Машина, ехавшая со скоростью 140 км/ч, при преследовании полицией увеличила скорость до 150 км/ч.

Таким образом, искусственный интеллект применяется в российском уголовном судопроизводстве для оказания составления документов, обработки статистических данных, наполнения сайтов правовой информацией правоохранительных органов и судов, обеспечения электронного доступа к материалам дел, обеспечение видеоконференцсвязи. Вместе с тем роль судьи в уголовном судопроизводстве должна оставаться весомой при принятии решения.

Список литературы

1. Апостолова Н. Н. Искусственный интеллект в судопроизводстве // Северо-Кавказский юридический вестник. 2019. № 3. С. 135–141.

2. Буряков П. Н. Искусственный интеллект и «предсказуемое правосудие»: зарубежный опыт // Lex russica. 2019. № 11. С. 79–87.

3. Колоколов Н. А. Компьютер вместо судьи – арифметика вместо души // Уголовное судопроизводство. 2019. № 3. С. 3–7.

4. Попова И. П. Автоматизация уголовного процесса: зло или благо для общества? // Мировой судья. 2019. № 11. С. 3–14.

5. Сушина Т. Е, Собенин А. А. Перспективы и риски использования искусственного интеллекта в уголовном судопроизводстве // Российский следователь. 2020. № 6. С. 15–21.

6. Черниговская Т. М. Цифровизация и человечность // Global Woman Media. 2020. URL: http://eawfpress.ru/presstsentr/news/glav/nauka/tatyana-chernigovskaya-tsifrovizatsiya-i-chelovechnost/ (дата обращения: 17.09.2022).

7. Kehl D., Kessler S. Algorithms in the criminal justice system: Assessing the use of risk assessments in sentencing. URL: http://nrs.harvard.edu/urn-3: HUL. InstRepos:33746041 (дата обращения: 17.09.2022).

8. Polloni C. Police prédictive: la tentation de ‘dire quel sera le crime de demain’. 2015. URL: https://www.nouvelobs.com/rue89/rue89-police-justice/20150527.RUE 9213/police-predictive-la-tentation-de-dire-quel-sera-le-crime-de-demain.html

9. Щелконогова Е. В. Цифровые технологии и уголовное право: вопросы взаимодействия // Вестник Югорского государственного университета. 2021. Вып. 1 (60). С. 105–110.

Н. В. Бушная,
кандидат юридических наук, заведующий кафедрой
общегуманитарных и юридических дисциплин,
Ставропольский филиал
Московского педагогического государственного университета
В. В. Кудинов,
кандидат педагогических наук, доцент,
Ставропольский филиал
Московского педагогического государственного университета

РИТОРИКА ЗАКОНОДАТЕЛЯ В ВОПРОСЕ ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ И КОПИРОВАНИЯ С НИХ ИНФОРМАЦИИ ПРИ ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Аннотация. Электронные носители информации, их изъятие и копирование с них сведений, имеющих непосредственное значение для расследования преступлений, являются лакмусом современных тенденций цифровизации, масштабного

использования IT-технологий в различных сферах, в том числе лицами, совершающими общественно опасные деяния с использованием указанных технологий. В статье анализируется взгляд законодателя в вопросе механизма приобщения электронных носителей информации, имеющей непосредственное отношение к расследованию преступления, результаты восприятия нововведений правоприменительной практикой, нуждаемость положений закона в совершенствовании.

Ключевые слова: информационное общество, электронный носитель информации, изъятие электронных носителей информации, копирование информации, цифровизация, доказательственное значение, использование специальных знаний, участие специалиста

THE RHETORIC OF THE LEGISLATOR ON THE ISSUE OF THE SEIZURE OF ELECTRONIC MEDIA AND COPYING INFORMATION FROM THEM DURING INVESTIGATIVE ACTIONS

Abstract. Electronic media, their seizure and copying of information directly relevant to the investigation of crimes from them are a litmus of modern trends in digitalization, large-scale use of IT technologies in various fields, including by persons committing socially dangerous acts using these technologies. The article analyzes the legislator's view on the issue of the mechanism of introducing electronic media directly related to the investigation of a crime, the results of the perception of innovations by law enforcement practice, the need for improvement of the provisions of the law.

Keywords: Information society, Electronic media, Seizure of electronic media, Copying of information, Digitalization, Evidentiary value, Use of special knowledge, Participation of a specialist

Информационное общество, цифровизация, информационные технологии – символы современного мирового и российского поступательного развития в сторону технического прогресса, направленного на взаимодействие общества и государства посредством технологий беспроводной передачи информации, искусственного интеллекта, возможности использования электронных платежных систем. Современные технологии буквально проникли в каждую сферу жизни общества, взаимодействия населения с органами власти, оказывая важное, а порой, решающее воздействие при принятии тех или иных решений в повседневной жизни и профессиональных областях [1. P. 2517]. Правовая сфера в этом вопросе не является исключением. Одной из тенденций цифровизации юридической деятельности является появление смарт-контракта, основанного на технологии блочных цепей (блокчейн), использование информационных технологий в различных видах судопроизводства, в том числе уголовно-процессуального.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы определяет основные ориентиры в механизме формирования общества знаний, возврата от так называемого клипового мышления к научному, образовательному уровню восприятия окружающего мира [12].

Отдельные из принципов указанного нормативного акта коррелируются со смысловым наполнением, сутью уголовного судопроизводства и выражаются

в обеспечении требований законности и разумности при проведении всех действий, связанных с получением информации о физических и юридических субъектах; гарантированности со стороны государства защищенности интересов российских граждан в информационной сфере.

Обеспечение национальных интересов, стратегических национальных ориентиров в развитии информационного общества корреспондируют международно-правовым актам, в частности, Окинавской хартии Глобального информационного общества, ставящей IT-технологии определяющим фактором формирования и развития общества двадцать первого века [10].

Цифровизация всех сфер жизнедеятельности общества и государства, необходимость использования цифровых ресурсов в праве, рост киберпреступности, сохранение важной для расследования преступлений информации на электронных носителях вынуждают законодателя на ответную реакцию в виде новелл, регламентирующих информационно-цифровую составляющую уголовного судопроизводства. Неизменным остается постулат о необходимости создания действенной системы гарантий прав участников уголовного судопроизводства по всевозможным вопросам, связанным с IT-технологиями.

Федеральный закон от 27.12.2018 № 533-ФЗ [5] видоизменил механизм нормативного регулирования в вопросах появления и использования в производстве по уголовным делам сведений, полученных с электронных носителей, добавив в ст. 164 УПК РФ ч. 4.1, а также введя новую норму 164.1. При этом из ст. 182 и 183 УПК РФ, регламентирующих, соответственно, производство обыска и выемки, были исключены части, содержавшие нормативные руководства по изъятию электронных средств и копированию с них информации.

Ключевым при анализе и толковании новелльных установлений является термин «электронный носитель информации». И здесь возникают определенные трудности ввиду отсутствия в уголовно-процессуальном законе легального определения, значимого именно для понимания такого объекта как составного компонента системы доказательств. Безосновательно было бы утверждать, что российское законодательство и система национальных стандартов не содержат каких-либо терминов, имеющих отношение к рассматриваемому вопросу. Например, УК РФ дает понятие компьютерной информации, Национальный стандарт РФ ГОСТ Р 7.0.8–2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» [11] так же, как и Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [7], обращаются к категории «электронный документ». Однако интересующий нас термин содержит только ГОСТ 2.051–2013 «Единая система конструкторской документации (ЕСКД). Электронные документы. Общие положения (с Поправкой)» [3], представляя его как материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники. Такая дефиниция перечисляет общие свойства без относительно и применительно к сфере уголовного судопроизводства, уделяющей особое внимание вопросам допустимости доказательств. Такая правовая неопределенность, в конечном итоге, может сказываться на результатах расследования и формировании доказательственной базы при расследовании преступлений.

Законодателю следует сосредоточить внимание на данном вопросе, что позволит исключить в правоприменительной практике возникновение ситуаций, нивелирующих результаты доказательственной деятельности следователей, дознавателей. Здесь следует согласиться с одной из точек зрения, делающей акцент на ключевое в содержании разрабатываемого понятия, а именно, на значимость получаемой информации для формирования доказательственной базы, а не на технические характеристики [4. С. 40].

Указанные выше нововведения сделали акцент на деяниях, затрагивающих предпринимательство. Предпринимательская деятельность является важным компонентом реализуемой национальной политики в силу значимости возлагаемых функции. Стратегия развития малого и среднего предпринимательства в Российской Федерации на период до 2030 г. [9] определяет функционал предпринимательства, имеющего целеназначением развитие интеллектуальной экономики, улучшение ее отраслевой структуры, обеспечение высоких показателей занятости населения.

Придавая особую значимость сфере предпринимательства, законодатель закрепляет гарантии защищенности от неправомерных действий должностных лиц в рамках уголовно-процессуальной деятельности, в частности, ч. 4.1. ст. 164 УПК РФ, закрепляет правило, запрещающее изъятие электронных средств без достаточных на то оснований. В следующей статье законодатель не забывает упомянуть об исключительных обстоятельствах. Речь идет о постановлении о назначении судебной экспертизы в отношении указанных объектов либо вынесенном судебном решении, предполагающим производство анализируемого процессуального действия.

Конструктивно непростым видится третье исключение в силу концентрации сразу нескольких исключающих возможности изъятия указанных носителей информации: их владелец не уполномочен на хранение и использование информации либо имеется альтернатива для ее использования в преступных целях или возможны утрата, изменение имеющейся на носителе информации, если будут проведены действия по ее копированию. В последнем утверждении вывод делает не сам следователь, а специалист. С данным суждением следует согласиться, поскольку действительно работа с техническими средствами, электронными носителями информации не проста, а требует специальных знаний, в противном случае, неумение или незнание технически верных действий может привести к утрате доказательственной базы. Правильный подход законодателя к регламентации правил, требований по вовлечению в сферу уголовно-процессуальной деятельности информации с электронных носителей, могущей быть преобразованной в доказательства, напрямую обусловливает качество расследования, решение задач уголовного судопроизводства.

Анализ перечисленных исключений свидетельствует о сложности восприятия для толкования и, самое главное, апробации правоприменителем анализируемых положений. Несомненно, появление таких положений неоднозначно было воспринято учеными-процессуалистами и представителями правоприменительной практики. Например, если речь идет о владельце электронного информационного средства, который не имеет соответствующих полномочий по ее хранению и использованию, то необязательно, с нашей точки зрения, что данные средства находятся у него в силу совершения им противоправных действий. Противоположной точки зрения

придерживается В. Ф. Васюков [2. С. 11], высказывающий именно этот аргумент как ключевой для данного исключения.

Предусмотренный п. 1 ч. 1 ст. 164.1 УПК РФ запрет на изъятие носителей информации электронного формата вызывает сомнение в возможности априори возникновения подобной ситуации.

Проведение любой экспертизы предполагает наличие объектов исследования, а не обратную последовательность, когда следователь выносит постановление, а потом ищет то, что будет исследоваться. Аналогично и в случае электронных доказательств: первично – изъятие носителя информации, вторично – вынесение постановление о назначении экспертизы, т. е. последнее может появиться в рамках уголовного дела уже тогда, когда проведено соответствующее следственное действие и изъят носитель информации, который в дальнейшем может выступать объектом экспертного исследования.

Второе исключение, предусмотренное п. 2 ч. 1 той же нормы уголовно-процессуального закона, вызывает неоднозначное толкование, что напрямую сказывается на формировании правоприменительной практики, демонстрирующей разноплановый подход к восприятию данной нормы. В каких случаях должно быть вынесено судебное решение, на основании которого может быть проведено процессуальное действие, сводящееся к изъятию электронных носителей информации? Решение суда носит «персонифицированный» характер относительно непосредственно носителя информации или касается следственного действия, которое предполагается производить с разрешения суда? Эти и многие другие вопросы, возникающие в уголовно-процессуальной деятельности правоохранительных органов, нередко либо создают препятствия для эффективного производства расследования, либо впоследствии приводят к признанию полученной информации недопустимой. В этом вопросе интересной видится пояснение Конституционного Суда РФ об отсутствии необходимости вынесения отдельного специального судебного решения для производства экспертизы, если изъятие абонентских устройств производилось в соответствие со всеми процессуальными требованиями. Если участники процесса не согласны с какими-то решениями или действиями должностных лиц, они могут их обжаловать в общем порядке, предусмотренном ст. 125 уголовно-процессуального закона [8].

Еще один вопрос, требующий внимания: распространяются ли установленные запреты на доследственную проверку сообщения о преступлении либо приобретают юридическую силу уже в рамках возбужденного уголовного дела? Согласно Постановления Пленума Верховного Суда Российской Федерации от 15 ноября 2016 г. № 48 [6], рассматривая поступившие жалобы на постановление о возбуждении уголовного дела, судом реализуется функция контроля, заключающаяся в проверке законности и обоснованности процессуальных действий, проведенных в ходе проверки сообщения о преступлении, обратив внимание на выполнение всех требований закона по изъятию электронных носителей информации. Такая рекомендация позволяет сделать вывод о возможности производства таких процессуальных действий до начала деятельности в рамках возбужденного уголовного дела и, следовательно, юридической силе установленных запретов на самом первоначальном этапе уголовно-процессуальной деятельности.

Риторика законодателя в отношении электронных носителей информации предполагает две составляющие: изъятие этих самых носителей и копирование с них информации. Изъятие, в свою очередь, требует соблюдение следующих условий: производство обусловленного обстоятельствами уголовного дела следственного действия и участие специалиста. Относительно последнего возникает вопрос: так ли необходимо привлечение сведущего лица в каждом случае проведения указанного процессуального действия? Возможно то, что данная норма является чрезмерной, не требующей привлечения специальных знаний и умений в каждом случае возникновения такой потребности. Считаем, что законодателю следует дополнить уточнением анализируемую норму о привлечении специалиста, когда по мнению следователя этого требует сама ситуация, что будет согласовываться с положениями закона о самостоятельности следователя как лица, ведущего расследование преступления.

Копирование информации представлено в двух вариациях: при изъятии электронного носителя и без такового. В последнем случае следователю предоставлено право самостоятельного копирования информации в ходе следственного действия. Данный случай, на наш взгляд, требует дифференцированного подхода в зависимости от сложности устройства электронного средства, содержащего необходимую информацию, с учетом обязательного исключения, уверенности, что данное действие не несет вреда расследованию. Отталкиваясь от данных факторов, должен решаться вопрос о привлечении лица, сведущего в этом вопросе, что согласуется с п. 3 ч. 1 ст. 164.1 УПК РФ, указывающей на необходимость получения мнения специалиста о запрете изъятия, поскольку это может привести к утрате или изменению интересующих следствие сведений.

Копирование информации, производимое при изъятии электронного носителя, не коррелируется с нормами ч. 2 ст. 82 УПК РФ и содержит противоречия. Указанное положение закона обращает внимание на производство действий по копированию информации локационно, а именно в помещении органа предварительного расследования или в здании суда, тогда как в ч. 2 ст. 164.1 такое уточнение отсутствует. Аналогичное рассогласование встречается и при толковании случаев запрета копирования информации: ч. 2 ст. 164.1 содержит отсылку к п. 3 ч. 1 этой же нормы, тогда как ч. 2.1 ст. 82 УПК РФ указывает на дополнительный запрет копирования сведений, если это будет препятствовать расследованию преступления. Объединяя все перечисленные случаи, получаем расширенную версию запретов копирования информации. Какая норма подлежит применению в данных обстоятельствах: общая или специальная либо следователь должен учитывать все исключения, перечисленные законодателем? Ответ на этот вопрос остается открытым.

Внимание законодателя должен привлечь вопрос о формировании соответствующей нормы с точки зрения конструктивного подхода. Семантика ст. 164.1 УПК РФ была бы более звучной при перестроении ее частей. На наш взгляд, по смыслу содержательной части правильней видится следование от общего к частному: первично описание порядка изъятия электронных носителей информации и копирования с них информации, а затем переход к тем запретам и ограничениям, которые в нынешней редакции содержатся в ч. 1 указанной нормы. При таком изменении ч. 2 и 3 станут, соответственно, 1 и 2, а ч. 1 будет завершать нормативную конструкцию.

Таким образом, пристальный анализ действий законодателя по внедрению регламентации относительно электронных носителей информации свидетельствует о необходимости доработки, модернизации, корректировки действующих положений, приведения ряда статей УПК РФ в соответствие друг с другом для исключения неоднозначной апробации в правоприменительной практике и, напротив, формирования ее единообразия.

Список литературы

1. Васюков В. Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. № 2. С. 8–14.

2. ГОСТ 2.051–2013 «Единая система конструкторской документации. Электронные документы. Общие положения (Введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. № 1628-ст). URL: https://docs.cntd.ru/document/1200106864?ysclid=l6ukykj7gg126409827

3. Григорьев В. Н., Максимов О. А. Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. 2019. № 2 (84). С. 33–44.

4. О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 27 декабря 2018 № 533-ФЗ // Российская газета. 29 декабря 2018. № 295.

5. О практике применения судами законодательства, регламентирующего особенности уголовной ответственности за преступления в сфере предпринимательской и иной экономической деятельности: Постановление Пленума Верховного Суда РФ от 15 ноября 2016 г. № 48 // Российская газета. 24 ноября 2016. № 266.

6. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Российская газета. 29 июля 2006. № 165.

7. Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Д. А. на нарушение его конституционных прав статьями 176, 177 и 195 УПК РФ: Определение Конституционного суда РФ от 25.01.2018 № 189-О. URL: https: www.ksrf.ru (дата обращения: 11.08.2022).

8. Об утверждении Стратегии развития малого и среднего предпринимательства в Российской Федерации на период до 2030 года (вместе с «Планом мероприятий («дорожной картой») по реализации Стратегии развития малого и среднего предпринимательства в Российской Федерации на период до 2030 года»): Распоряжение Правительства РФ от 02.06.2016 № 1083-р (ред. от 30.03.2018) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_199462/ (дата обращения: 11.08.2022).

9. Окинавская хартия Глобального информационного общества // Дипломатический вестник. 2000. № 8.

10. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения: национальный стандарт

РФ ГОСТ Р 7.0.8–2013 (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 октября 2013 г. № 1185-ст). URL: https://docs.cntd.ru/document/1200108447?ysclid=l6ukecn684210777985 (дата обращения: 11.08.2022).

11. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

12. Balashova A. Action Plan For Using Digital Evidences When Investigating Drug Marketing Via The Internet, Instant Messengers And Crypto markets / A. Balashova, V. Vasyukov, O. Efremova, G. Gasparyan // Jour of Adv Research in Dynamical & Control Systems. 2019. Vol. 11. Spesial Issue-08. Pp. 2517–2524.

Ю. В. Быстрова,
доктор юридических наук, доцент,
Орловский государственный университет имени И. С. Тургенева
Е. Е. Быстрова,
студент Банковского колледжа
Среднерусский институт управления, филиал Российской академии народного хозяйства и государственной службы при Президенте РФ
В. С. Изотова,
магистр,
Орловский государственный университет имени И. С. Тургенева

ТАКТИКА ПРОИЗВОДСТВА ВЕРБАЛЬНЫХ И НЕВЕРБАЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. В статье рассматриваются актуальные проблемы, возникающие при расследовании киберпреступлений. Исследована система средств, с помощью которых совершаются данные виды преступных деяний: электронная почта, файловые архивы, видеоблоги, носители информации (персональные компьютеры, ноутбуки, оптические диски, умные часы, смарт-браслеты, смартфоны и т. д.). Предложено оптимальное сочетание вербальных и невербальных методов, способствующих быстрому раскрытию и расследованию рассматриваемых деяний.

Ключевые слова: компьютерные преступления, киберпреступления, компьютерные средства, компьютерные технологии, вербальные и невербальные следственные действия

TACTICS OF VERBAL AND NON-VERBAL INVESTIGATIVE ACTIONS IN THE INVESTIGATION OF CYBERCRIMES

Abstract. The article discusses the current problems arising in the investigation of cybercrimes. The system of means by which these types of criminal acts are committed is investigated: e-mail, file archives, video blogs, information carriers (personal computers, laptops, optical disks, smart watches, smart bracelets, smartphones, etc.), an optimal combination of verbal and non-verbal methods that contribute to the rapid disclosure and investigation of the acts in question is proposed.

Keywords: Computer crimes, Cybercrimes, Computer tools, Computer technologies, Verbal and non-verbal investigative actions

Актуальность выбранной темы обуславливается тем, что проблема информационной безопасности является одной из ведущих в современном обществе. Как указывают исследователи, Россия является одной наименее защищенных от киберугроз стран, что приводит к массированным атакам на экономику, политику, общественную жизнь. Большая часть совершаемых преступлений обусловлена обострением идеологической борьбы и тем давлением, которое западный мир оказывает на Россию. Именно поэтому в настоящее время специалисты в области юриспруденции особенно активно обращают внимание на изучение киберпреступлений и механизмов борьбы с ними. Важным является и то, что данный вид преступлений направлен не только против безопасности страны, но и частной жизни гражданина.

В УК РФ [1] дается достаточно точная классификаций преступлений и ответственности, которая предусмотрена ст. 272–274 гл. 28 УК РФ. Однако определение киберпреступления, как общественно опасного деяния, отсутствует. В научной литературе также не существует единой точки зрения на содержание понятия. В. Б. Вехов, Ю. И. Ляпунов, Н. А. Селиванов используют термин «компьютерные преступления», хотя и считают, понятие применимо только к криминологическому и криминалистическому аспектам. М. Ю. Дворецкий, В. А. Копылов, В. В. Крылов, В. А. Пархомов предлагали использовать термин «информационные преступления». И. Н. Соловьевым предложен термин «преступление, совершенное в киберпространстве» [6. С. 64]. И. А. Петрова и И. А. Лобачев считают целесообразным называть киберпреступления «преступлениями в сфере компьютерной (цифровой) информации» [4. С. 56].

Наиболее приемлемым является определение, предложенное Д. Н. Карповой: «Киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет» [3. С. 48].

Предложенное исследователем определение отражает основные аспекты преступлений, совершаемых в интернет-пространстве, и подчеркивает, что киберпреступления могут охватывать все стороны общественных отношений и распространятся на все слои общества, государственные структуры, предприятия и организации. Однако данное определение следует дополнить уточнением, что к киберпреступлениям следует относить не только преступные деяния, связанные с обработкой, хранением или передачей компьютерной информации, но и «любые преступные посягательства, совершаемые с применением информационно-коммуникационных технологий» [5. С. 104].

Определенный интерес представляют научные концепции ученых (Ю. М. Батурин и А. М. Жодзишский), которые считают, что киберпреступлений как самостоятельного вида не существует, а все деяния в киберпространстве должны квалифицироваться по общеуголовным статьям. С. Ю. Бытко прямо указывает на то, что природа преступлений, совершаемых в киберпространстве, принципиально не меняется, хищение остается тайным хищением чужого имущества, мошенничество

остается мошенничеством, доведение до самоубийства полностью соответствует положениям ст. 100 УК РФ, а кража рассматривается не только, как преступление, связанное с кибертехнологиями, но и по ст. 158. Исследователь указывает на «нежизнеспособность выбранной концепции и необходимость возврата к прежним представлениям, согласно которым процессы передачи и обмена информацией выступают в качестве вспомогательных и не могут претендовать на роль самостоятельных общественных отношений» [2. С. 18].

Данная научная позиция не лишена смысла, так как к киберпреступлениям относятся преступления, предусматривающие наказания по ст. 146, 159, 242 УК РФ и т. д.

Об этом свидетельствует и судебная практика. Так, в Постановлении от 5 августа 2013 г. по делу № 10–7098 Московского городского суда преступления квалифицировались по ч. 2 ст. 146 и ч. 2 ст. 273 УК РФ, Постановлением от 20 апреля 2015 г. № 44У-6/2015 Президиума Курганского областного суда в отношении Д. применены ч. 2 ст. 158 УК РФ и ст. 273, в Апелляционном определении № 10–86/2014 Челябинского областного суда оставлена мера пресечения в отношении Н., осужденного по ч. 2 ст. 146 УК РФ и ч. 3 ст. 273 УК РФ и т. д. Следовательно, можно согласиться с тем, что преступления, совершаемые в сети Интернет, рассматриваются в качестве вспомогательных.

Разрешение возникающей дилеммы возможно только при анализе тактики производства вербальных и невербальных следственных действий при расследовании киберпреступлений, что и составляет цель нашего исследования. При расследовании преступлений, совершаемых с помощью кибертехнологий, исследуется такие средства, как электронная почта, тестовые сообщения, телеконференции, файловые архивы, узлы удаленного управления компьютерами, видеоблоги, интернет-журналы, онлайн-дневники и носители информации (персональные компьютеры, ноутбуки, планшеты магнитные диски, жесткие диски, дискеты, гибкие диски, оптические диски, переносные накопители данных, умные часы, смарт-браслеты, смартфоны, маршрутизаторы), а так же механизмы преступлений, совершаемых с использованием компьютерных средств и систем.

Соответственно с криминалистической точки зрения расследование данных преступных деяний заключается в собирании и исследование материалов доказательственного характера о совершенном преступлении, тех цифровых следов, которые оставляет деятельность с использованием компьютерных технологий.

Общеизвестно, что при расследовании уголовных дел большая часть рабочего времени следователя при проведении следственных действий расходуется на подготовку и производство вербальных следственных действий (по некоторым данным 68,4 % от общего времени). Вербальные действия обусловлены тем, что в их основе лежит устная речь. Соответственно, допросы свидетеля, потерпевшего, подозреваемого, обвиняемого (подсудимого), эксперта, специалиста и очные ставки традиционно выступают как основное средство собирания и проверки доказательственной информации. Цели допроса и очной ставки заключаются в психологическом воздействии на допрашиваемого, стремлении склонить его на сторону правосудия, пробудить его гражданскую совесть. Тактика использования вербальных приемов заключается в детализации события преступления, выстраивании аналогий, когда

следователь предлагает вспомнить не само течение преступления, а сходные процессы, сопутствующие явления, наглядности, заключающейся в демонстрации конкретных примеров.

Одним из широко распространенных тактических приемов является применение криминалистической фоноскопии, которая заключается в том, что по зафиксированному на электронном носителе голосовому следу проводится идентификация личности. Кроме того, фонограммы «как результат контроля и записи телефонных и иных переговоров, приобщаемые к материалам уголовных дел, служат одним из доказательств, имеющих существенное значение для их раскрытия и расследования» [7. С. 104] уголовного преступления. При анализе записанной речи выявляются изменения тембра голоса, его устойчивости/отсутствии ритмичности дыхания, наличии/отсутствии стереотипных фраз.

Применение криминалистической фоноскопии особенно важно при расследовании киберпреступлений. Данные тактические приемы приобретают особую значимость при расследовании преступлений в интернет-пространстве, так как позволяют провести идентификацию лица, совершившего преступление, по голосу в тех случаях, когда устная речь звучит за кадром, комментирует или интерпретирует визуальный ряд.

В качестве доказательной базы зафиксированное в интернет-пространстве преступление выступает после проведения фоноскопической экспертизы и является достаточно эффективным средством воздействия на подследственное/обвиняемое лицо.

В настоящее время существуют сотни программ по изменению голоса. Самыми распространенными и, по сути, общедоступными являются AV Voice Changer (три уровня Basic, Gold и Diamond), Voxal Voice Changer, MorphVOX JR, MorphVOX, Pro Scramby, Fake Voice, Funny Voice, Clownfish Voice Changer и т. д. С помощью данных программ изменяется тон голоса, его высота, регистр, голос может изменяться по половому признаку, роботизироваться. Однако после приведения записи к исходному состоянию, она выступает в качестве неопровержимой улики. И в этом заключается принципиальное отличие в расследовании ряда киберпреступлений от записей, сделанных с помощью скрытой камеры, микрофона, записи телефонного разговора. Подобного рода записи в соответствие со ст. 23, 24 Конституции РФ судом не рассматриваются и к материалам судебного дела не приобщаются. Интернет же является публичным пространством, поэтому зафиксированные материалы могут использоваться следственными органами при раскрытии и квалификации уголовного преступления.

В том случае, когда программа по изведению звучащей речи выполнена на высоком уровне и не поддается приведению к исходному материалу, прибегают в лингвистической экспертизе, которой устанавливаются наиболее частотные, стереотипные высказывания носители речи, причем учитывается не столько фонетический ряд, сколько супрасегментная составляющая, т. е. целые синтаксические отрезки речи.

Доказывание преступлений с применением невербальных тактик направлено на производство и обработку компьютерных средств (носителей информации) и самой информации. Действия следственны органов направлены на изучение способов совершения преступления, фиксацию электронных носителей, их осмотр и изъятие

на месте преступления. В том случае, если информация удалена с электронных носителей, обнаруженных на месте преступления, то изучаются цифровые следы, проводится анализ данных, сохраняемых в оперативной памяти.

Невербальные тактики следственных действий предусматривают поиск и фиксацию той информации, которая может быть обнаружена на рабочем месте преступника. Поэтому первичными при осмотре места преступления становится осмотр электронных носителей информации и компьютерных устройств, проведение проверки сетевых подключений, изучение информации, в сохраненных файлах и оперативной памяти, создаются копии жесткого диска и производится отключение компьютера и всех внешних устройств. После завершения осмотра места преступления следственные действия проводятся неработающей системой, т. е. изучается информации, удаленная с материального носителя.

Наибольшие трудности в осуществлении раскрытия киберпреступлений связаны с расследованием, которое проводится на уровне сетевых ресурсов, фиксирующих информацию в локальной или глобальной сетях. Следственные действия предусматривают осмотр компьютерной системы в целом с учетом того, что преступление может совершаться не только в разных помещениях, зданиях, но и в различных регионах. В таком случае изучаются провайдеры, представляющие сетевые ресурсы, процессы передачи информации, которые осуществлялись в сети, начиная от рабочей станции, к цепочке компьютеров и серверов и до устройств, являющихся непосредственными инструментами преступления.

Таким образом, изученные источники, материалы практической деятельности следственных органов, материалы решений, вынесенных судами РФ, позволяют сделать вывод о правомерности включения в Уголовный кодекс РФ гл. 28, предусматривающей наказание за совершение киберпреступлений. Расследование данных преступлений имеет специфическую тактику вербального и невербального производства следственных действий, которые заключается в исследовании как систем – носителей информации, так и средств, фиксирующих информацию.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в редакции от 28.06.2022) // СПС «КонсультантПлюс».

2. Бытко С. Ю., Митькин С. Б. Правовая информационная система «ДРАКОН-право» на базе алгоритмического визуального языка «ДРАКОН» // Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций: коллективная монография. В 2 т. Т. 1 / под ред. Н. Н. Ковалевой. Саратов: Изд-во ФГБОУ ВО «Саратовская государственная юридическая академия», 2020. С. 322–335.

3. Киберпреступления – 21 века. URL: https://blog.studylie.ru/kiberprestuplenija-problema-21-veka (дата обращения: 28.06.2022)

4. Петрова И. А., Лобачев И. А. Преступления в сфере компьютерный (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований, 2020. № 1. С. 52–62.

5. Россинская Е. Р., Рядовский И. А. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Lex Russic, 2021. Т. 74, № 9 (178). С. 102–116.

6. Уголовно-правовые риски в условиях цифровизации: способы противодействия от 02.02.2021. URL: https://www.garant.ru/news/1443692/ (дата обращения: 28.06.2022).

7. Аносов А. В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие в 2 ч. Москва: Академия управления МВД России, 2019. Ч. 1. 208 с.

Э. Р. Гафурова,
кандидат юридических наук, доцент,
Удмуртский государственный университет

ОСОБЕННОСТИ ПРИМЕНЕНИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Искусственный интеллект становится неотъемлемой частью в развитии современного постиндустриального общества, поэтому необходимо обеспечить должное правовое регулирование его использования, а также меры ответственности, применяемые в случае нарушения закона. В данной статье проводится анализ субъектов совершения противоправных деяний с использованием искусственного интеллекта, искусственный интеллект рассматривается как орудие совершения преступления, предлагаются возможные пути совершенствования законодательства в целях эффективного применения искусственного интеллекта.

Ключевые слова: уголовная ответственность, цифровые технологии, искусственный интеллект, освобождение, субъект преступления, орудие преступления, преступление

FEATURES OF THE APPLICATION OF CRIMINAL LIABILITY IN THE USE OF ARTIFICIAL INTELLIGENCE

Abstract. Artificial intelligence is becoming an integral part in the development of modern post-industrial society, therefore it is necessary to ensure proper legal regulation of its use, as well as measures of responsibility applied in case of violation of the law. This article analyzes the subjects of committing illegal acts using artificial intelligence, artificial intelligence is considered as a tool for committing a crime, and possible ways to improve legislation for the effective use of artificial intelligence are proposed.

Keywords: Criminal liability, Digital technologies, Artificial intelligence, Liberation, Subject of crime, Instrument of crime, Crime

Процесс развития искусственного интеллекта (далее – ИИ) ежедневно набирает обороты не только в сфере цифровых технологий, но и в системе российского права.

Зачастую мы сталкиваемся с ИИ в нашей жизни, по своей природе он способен относительно автономно решать различного рода задачи. Например, искать оптимальный маршрут действий (Siri, Алиса), находить новые знакомства («ВКонтакте»), консультировать (голосовой помощник Альфа-банка) и т. д.

ИИ – это не что иное, как феномен, который предстает перед человеком в виде реальных (осязаемых) продуктов или устройств [2. С. 39].

З. И. Хисамова и И. Р. Бегишев в своем научном исследовании ИИ указывают на то, что в процессе применения ИИ возможно возникновение четырех определенных ситуаций, требующих уголовно-правового регулирования:

– при разработке и создании системы ИИ была допущена ошибка, которая привела к совершению преступления;

– в систему ИИ был осуществлен неправомерный доступ, повлекший повреждение или модификацию его функций, вследствие чего было совершено преступление;

– ИИ, обладающий способностью к самообучению, принял решение о совершении действий либо бездействия, квалифицируемых как преступление;

– ИИ был создан преступниками для совершения преступлений [4. С. 567].

Соглашаясь с мнением З. И. Хисамовой и И. Р. Бегишева, следует неоспоримый вывод о том, что ИИ следует рассматривать как субъекта совершения преступления. Однако, ст. 19 Уголовного кодекса Российской Федерации (далее – УК РФ) гласит, что субъектом совершения преступного деяния может быть только физическое лицо [1].

В соответствии с этим возникает вопрос, как быть правоприменителям при установлении субъекта преступления.

По нашему мнению, так как субъектом преступления, в соответствии с действующим уголовным законодательством, не может быть ИИ, возможно его стоит рассматривать в качестве орудия совершения преступления.

Так, доктор юридических наук А. И. Рарог рассматривает орудия совершения преступлений, как предметы материального мира, приспособления, применяемые для усиления физических возможностей лица, совершающего общественно опасное деяние [3. С. 98].

Исходя из вышеизложенного необходимо определить, что ИИ в соответствии с нормами российского уголовного законодательства должен рассматриваться как орудие совершения преступлений, соответственно ответственность за совершенные противоправные действия должна применяться к физическому лицу относительно его участия в создании, разработке или применении ИИ.

Действительно, уникальные особенности ИИ, обеспечивающие сложность модификации путем обновления либо же самообучения и ограниченную предсказуемость, могут в дальнейшем затруднить процедуру определения того, что пошло не так, и кто должен нести ответственность, если это произойдет.

Потому как в процессе подготовки ИИ к применению или же действительному применению, как правило, участвует много сторон в виде поставщика информационных данных, проектировщика, программиста, разработчика, пользователя и т. д.

Ответственность указанных лиц за совершенные преступные деяния должна наступать в зависимости от этапа, на котором было совершено такое преступление. К примеру, если в случае использования ИИ в работе с персональными данными произошла утечка информации, относящейся к определенному лицу, то следует рассматривать возможность привлечения к уголовной ответственности непосредственно

к лицу, применяющему ИИ в своей деятельности. Если же ошибки произошли на этапе создания работы ИИ, то в таком случае ответственность должна применяться в отношении разработчиков (программистов).

Поскольку на сегодняшний день правовое регулирование ИИ разрабатывается и совершенствуется, разумно предусмотреть альтернативную меру для субъектов совершения преступлений с использованием в качестве орудия ИИ в виде смягчающих обстоятельств, а также освобождения от уголовной ответственности указанных лиц.

Таким образом, в качестве смягчающих обстоятельств предусмотреть совершение преступления с использованием ИИ, данную меру закрепить путем внесения изменений в виде нового п. «л» в ч. 1 ст. 61 УК РФ.

Соответственно закрепить в качестве основания освобождения от уголовной ответственности в гл. 11 УК РФ норму, регламентирующую условия, при которых лицо может быть освобождено от ответственности в связи с использованием ИИ.

Рекомендуется закрепить указанное законодательное предложение путем включения в гл. 11 УК РФ новой ст. 76.3 «Освобождение от уголовной ответственности в связи с использованием ИИ», предусматривающей, что лицо, впервые совершившее преступление небольшой или средней тяжести, может быть освобождено от уголовной ответственности, если преступление было совершено с использованием ИИ, являющихся орудием (средством), а также, если лицо активно способствовало раскрытию и расследованию такого преступления, в полном объеме возместило ущерб либо иным образом загладило вред, причиненный этим преступлением.

Подводя итог вышеизложенному, отметим, что указанные предложения по совершенствованию законодательства будут способствовать развитию правового закрепления и регулирования ИИ, а также определят ответственность субъектов отношений во взаимосвязи с ИИ, позволят защитить их от несправедливого обвинения и наказания.

В подтверждение приоритета регулирования ИИ Президент Российской Федерации справедливо указал: «Важно, чтобы такие прорывные решения, открывающие поистине безграничные возможности, работали не во вред ни в коем случае, а на благо человека, помогали сберечь планету, обеспечить ее устойчивое развитие». Поэтому, несмотря на прогрессивное развитие ИИ требуется обязательно обеспечить их должное правовое регулирование, в целях развития современного государства и общества.

Список литературы

1. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ // Российская газета. № 113. 1996.

2. Резаев А. В., Трегубова Н. Д. «Искусственный интеллект», «Онлайн-культура», «Искусственная социальность»: определение понятий // Мониторинг общественного мнения: Экономические и социальные перемены. 2019. № 6. С. 35–47.

3. Уголовное право России. Части Общая и Особенная: учебник / под ред. А. И. Рарога. 10-е изд. Москва: Проспект, 2018. 841 с.

4. Хисамова З. И., Бегишев И. Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты // Всероссийский криминологический журнал. 2019. Т. 13, № 4. С. 564–574.

Д. В. Голенко,
кандидат юридических наук, доцент,
Самарский национальный исследовательский
университет имени С. П. Королева

ОСОБЕННАЯ ЧАСТЬ УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ И ЦИФРОВЫЕ ТЕХНОЛОГИИ

Аннотация. Цель исследования состоит в установлении объема регулирования Особенной часть УК РФ отношений, связанных с цифровыми технологиями. Современная Особенная часть отечественного уголовного законодательства не использует понятие «цифровые технологии», но в определенной степени регулирует отношения, возникающие в результате использования таковых. Актуальным является вопрос о том, каким признаком состава преступления являются цифровые технологии, а также имеются ли предпосылки для объединения группы посягательств на цифровые технологии в самостоятельный структурный компонент Особенной части УК РФ. Отношения, связанные с цифровыми технологиями, новый вызов для современного права. Законодателю важно найти компромисс между соблюдением и защитой прав человека, защитой безопасности личности, общества и государства, и не препятствованию развития этой современной отрасли.

Ключевые слова: Особенная часть Уголовного кодекса, цифровые технологии, уголовный закон, информационно-телекоммуникационные сети, структура уголовного закона

SPECIAL PART OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION AND DIGITAL TECHNOLOGIES

Abstract. The article is devoted to establishing the scope of regulation of the Special Part of the Criminal Code of the Russian Federation of relations related to digital technologies. The modern Special Part of the domestic criminal legislation does not use the concept of “digital technologies”, but to a certain extent regulates relations arising from the use of such technologies. Relevant is the question of what sign of a crime are digital technologies, and whether there are prerequisites for combining a group of infringements on digital technologies into an independent structural component of the Special Part of the Criminal Code of the Russian Federation. Relationships related to digital technologies, a new challenge for modern law. It is important for the legislator to find a compromise between observance and protection of human rights, protecting the security of the individual, society and the state, and not hindering the development of this modern industry.

Keywords: Special part of the criminal code, Digital technologies, Criminal law, Information and telecommunication networks, Structure of the criminal law

Введение. Цифровые технологии становятся неотъемлемой часть повседневной жизни человека. Документооборот, денежные обороты, и даже ведение домашнего хозяйства в современном мире осуществляются с использованием цифровых технологий. С одной стороны цифровые технологии облегчают жизнь, сокращают время, используемое для решения различных задач, но с другой стороны ставят новые

вызовы для различных областей, в том числе, и права. Соблюдение прав человека, обеспечение безопасности личности и сохранение ее персональных данных, защита юридических лиц, безопасности государства в условия стремительного развития цифрового пространства является одной из задач, которую предстоит решить науке. Важным является оценка пределов вмешательства уголовного законодательства в регулирование общественных отношений, возникающих в связи с применением, созданием, использованием цифровых технологий.

Основная часть. Обозначим некоторые проблемы регулирования использования, создания цифровых технологий в Особенной части УК РФ.

Сформулируем вопрос: «Регулирует ли Особенная часть УК РФ в настоящее время отношения, связанные с цифровыми технологиями?». Ответ на него зависит от того, что понимать под «цифровыми технологиями». В настоящее время законодатель не использует это понятие в уголовном кодексе, но используются иные, близкие категории. Например, в качестве квалифицирующего признака в некоторых статьях УК РФ названо использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» (ст. 128.1 УК РФ), использование электронных средств платежа (ст. 159.3 УК РФ) и др. Отдельная глава посвящена преступлениям в сфере компьютерной информации (глава 28 УК РФ). И хотя в доктрине указывается, что появляются «отдельные главы УК РФ, призванные регулировать и охранять вновь возникающие правоотношения» (имеются в виду отношения, связанные с цифровыми технологиями) [2. С. 109], на самом деле, с момента принятия УК РФ число и название разделов и глав в Особенной части не изменялось.

До настоящего времени не решен вопрос как соотносятся понятия «информационные технологии», «цифровые технологии», «компьютерная информация» и другие близкие понятия. Помимо «цифровых технологий» в доктрине предлагается использовать и иные понятия, например, «кибернетические технологии» [1. С. 109]. Озвучивание различных современных терминов, понятий скорее обозначают проблему, чем ее решение. Сложно регулировать то, что не определено в содержательном плане. Законодатель находится в поиске понимания даже тех понятий, которые уже используются в Особенной части УК РФ с 1996 г. Так, например, если в 1996 году в УК РФ понятия «компьютерная информация» была связана с машинным носителем, ЭВМ. То современный законодатель уже не использует в раскрытии содержания понятия «компьютерная информация» такие категории как «машинный носитель», «ЭВМ». Хотя электронно-вычислительные машины называются, например, среди специальных технических средств (ст. 138.1 УК РФ). Если на момент принятия УК РФ актуальным вопрос был о компьютере как ЭВМ, то сейчас возникает вопрос что такое современный компьютер, как он соотносится, например, со смартфоном, электронными часами и др. техническими средствами, способными создавать, перерабатывать, передавать, хранить информацию. Все чаще встает вопрос о том, что такое цифровой объект. Например, в науке является дискуссионным вопрос о том, является ли отсканированный документ цифровым документом и т. д.

Решением проблемы является законодательное закрепление понятий, используемых при создании, применении и других действиях, связанных с цифровыми технологиями, информационными технологиями. Необходимо установить соотношение понятий, связанных с цифровым пространством. Если такое законодательство

будет разработано и принято, то необходимости дополнительно определять содержание и соотношение этих понятия в Особенной части УК РФ отпадет. Бланкетные диспозиции статей давно и успешно используются современным законодателем.

Относительно необходимости объединения посягательств на отношения, связанные с цифровыми технологиями, вопрос дискуссионный. Необходимо определиться к какому элементу состава преступления они относятся. Цифровые технологии можно рассматривать как средство совершения преступления, в некоторых случаях как способ. Возможно, цифровые технологии могут быть объектом уголовно-правовой охраны, но скорее речь идет не о самих технологиях, а о безопасности личности, общества, государства в этом новом для человечества пространстве – цифровом. Некоторые ученые озвучивают и введение цифровых технологий в элемент субъекта преступления, когда речь идет об искусственном интеллекте. Однако вряд ли можно говорить об искусственном интеллекте как субъекте преступления в современном понимании этого элемента преступления.

В настоящее время нет предпосылок для объединения посягательств на отношения, связанные с цифровыми технологиями, в структурный компонент Особенной части УК РФ. Не обозначена та группа преступлений, которые возможно было бы объединить как посягательства с единым объектом – отношения, связанные с цифровыми технологиями. Но есть основания размышлять над кругом преступных деяний, которые сейчас объединены в главе 28 УК РФ, а возможно, существующих пробелах в регулировании новых отношений, а также над тем, актуально ли в настоящее время использование понятия «компьютерная информация».

Заключение. Для современного уголовного законодательства важным является определение пределов регулирования отношений, возникающих в результате применения (создания, использования) цифровых технологий. Это регулирование должно в себе сочетать два важных аспекта: не препятствовать развитию цифровых технологий; не создавать реальные угрозы безопасности личности, общества, государства, не нарушать права и свободы человека. Для уголовного права необходимо определиться являются ли цифровые технологии объектом преступления, выступают в качестве признака объективной стороны (например, способа или средства совершения преступления или иного признака). Если признать цифровые технологии объектом уголовно-правовой охраны, то какие посягательства являются преступными и необходим ли структурный элемент внутри Особенной части УК РФ для их объединения. Это лишь некоторые вопросы, которые может сформулировать современный исследователь. Думается, что с развитием цифрового пространство вопросы о криминализации и декриминализации посягательств, связанных с цифровыми технологиями, не будут утрачивать своей актуальности и необходимости своевременного и корректного решения.

Список литературы

1. Пучков Д. В. Кибернетические технологии в социально-биологической сфере: уголовно-правовые аспекты: монография. Москва: Юрлитинформ, 2020. 200 с.

2. Щелконогова Е. В. Цифровые технологии и уголовное право: вопросы взаимодействия // Вестник Югорского государственного университета. 2021. Вып. 1 (60). С. 105–110.

Н. Н. Гончарова,
кандидат юридических наук,
Казанский инновационный университет им. В. Г. Тимирясова

ПРАВОВАЯ ПОМОЩЬ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Аннотация. В данном исследовании проведена попытка постановки задачи актуализировать развитие цифрового права с целью расширения основы оказания правовой помощи в условиях использования виртуального пространства. Эта возможность рассматривается в качестве меры эффективной реализации прав и свобод человека, неспособного преодолеть вызовы современной геополитики.

Ключевые слова: виртуальное пространство, права человека, правовая помощь, внешние сношения, цифровые технологии

LEGAL ASSISTANCE WITHIN THE FRAMEWORK OF THE VIRTUAL SPACE

Abstract. In this study, an attempt was made to set the task of actualizing the development of digital law in order to expand the basis for providing legal assistance in the context of using virtual space. This possibility is considered as a measure of effective implementation of the rights and freedoms of a person who is not able to overcome the challenges of modern geopolitics.

Keywords: Virtual space, Human rights, Legal assistance, External relations, Digital technologies

В сентябре 2022 г. прошла 77-я сессия Генеральной Ассамблеи ООН, по результатам которой были расставлены актуальные приоритеты и сформулированы задачи в поиске решений на основе солидарности, устойчивого развития и науки.

Относительно недавно членами ООН была принята «Повестка дня в области устойчивого развития до 2030 г.», в которой был закреплен ряд принципов и целей, среди которых предлагается развитие помощи государств на основе взаимности, открытости, равного доступа к правосудию и др. Успешная и эффективная реализация указанных целей зависит от сотрудничества правительств государств на универсальном, региональном, а также двустороннем уровне.

В рамках развития межгосударственных внешних сношений достаточно интересен вопрос о гарантиях реализации прав и свобод человека при совершении уголовно-процессуальных действий, в том числе с участием иностранных граждан. Такие гарантии стоит расширить и развить до цифрового уровня, при условии распространения их в виртуальном пространстве.

Возникает вопрос: возможно ли использовать такое пространство для проведения различного рода следственных действий должностными лицами России и по праву России, прежде всего в тех случаях, когда в результате имеет интерес каждый отдельно взятый участник, в том числе запрашивающий правовую помощь. В одном из исследований была допущена вероятность проведения уголовно-процессуальных действий в рамках учреждений внешних сношений в аналогичных целях [1].

В обозначенной Программе ООН актуализировало содействие в вопросах сотрудничества и совместной деятельности в том числе по направлениям внешних сношений. В духе сотрудничества предполагается также соблюдение основополагающих принципов, таких как равенство суверенитетов, добросовестного выполнения взятых международных обязательств, невмешательство во внутренние дела и других. Только учитывая незыблемые начала, стоит строить систему методов проведения мер правовой помощи при помощи цифровых технологий.

Физические лица активно вступают в различные экстерриториальные правоотношения в гражданской, семейной, уголовной сферах. Причем место в структуре правоотношений для таких лиц различное: заявитель, потерпевший, свидетель и др.

Согласно ч. 1 ст. 3 УПК РФ, производство по уголовным делам о преступлениях, совершенных иностранными гражданами, осуществляется в рамках УПК, соблюдение которого является обязательным для каждого, в том числе участвующего апатрида или иностранного гражданина.

Действующие нормы не предусматривают возможность использования в рамках правовой помощи средств виртуального общения, хотя такая необходимость надиктована современным мироустройством, а человек, действуя в своих интересах в рамках уголовного или иного процесса, вынужден добиваться права пересечь государственную границу своего и иностранного государства. Данная проблема легко может быть решена при признании виртуального способа в качестве возможного для проведения, например, следственных действий по допросу свидетеля, потерпевшего или иного заинтересованного в расследовании преступления дела.

Действительно, на данный момент интернет-пространство уже является своеобразной площадкой для заключения сделок с иностранным элементом, подачи жалобы, выставления претензии и т. д.

Действующее международное право не предусматривает, но и не запрещает действия процессуального характера в сети Интернет, однако это только порождает неуверенность и осторожность при возможном обращении к такому способу коммуникации.

Откровенную сложность представляет действительный вызов на допрос иностранного гражданина, запланированный в рамках виртуального пространства, ввиду того, что фактически лицо будет в момент такого следственного действия находиться за пределами Российской Федерации, значит, технически это порождает препятствие для применения уголовно-процессуального законодательства России. Однако возможно рассмотреть использование привязки его к праву места вызова на допрос, или места составления процессуального акта, или проведения другого действия, имеющего юридическое значение, в том числе для разрешения спора.

Стоит выразить также озабоченность в обязательном и неукоснительном соблюдении правила о добровольном участии заинтересованных сторон в процессуальных действиях, проводимых в виртуальном пространстве. Так, Европейская конвенция о взаимной правовой помощи по уголовным делам закрепляет правило о согласии иностранца на проведение следственных действий, если есть сомнения в необходимости проводимого действия в рамках правовой помощи.

Неуверенность в допустимости современных технологий к проведению уголовно-процессуальных действий можно легко преодолеть путем развития права и расширения соответствующего уровня правосознания.

Выводы. Приведем в систему основные тезисы и предложения по повышению эффективности и развитию устойчивого развития правовой помощи:

1. В нормах международного права нет правил использования цифровых технологий для проведения мероприятий в рамках правовой помощи.

2. Виртуальное пространство может стать площадкой для правовой помощи. Данная возможность направлена на реализацию прав и свобод человека, не имеющего возможности прибыть в страну для участия в уголовно-процессуальных действиях.

При оказании правовой помощи в уголовном процессе необходима четкая определенность порядка использования виртуального пространства, в частности соблюдение принципов согласия участника, надлежащее уведомление о способах контакта при помощи цифровых технологий и др.

Проблема применения права России, тогда как виртуальное пространство не рассматривается в юрисдикционном контексте в действующем праве, что вызывает необходимость восполнения пробела в праве.

Представляется возможным начать разработку проекта закона, регулирующего вопросы эффективного использования виртуального пространства и цифровых технологий для реализации целей внешних сношений и правовой помощи прежде всего в уголовных делах. Такая необходимость обусловлена целями устойчивого развития наиболее перспективных направлений деятельности человечества через упрощение процедур проведения ряда следственных действий при помощи современных технологий.

Список литературы

1. Гончарова Н. Н. Проблемы проведения уголовно-процессуальных действий с участием иностранных граждан, на российской территории, а также в зданиях посольств и консульств России / Н. Н. Гончарова, Э. Ю. Латыпова, Н. А. Гончаров // Пробелы в российском законодательстве. 2021. Т. 14, № 4. С. 366–372.

Д. В. Горбань,
кандидат юридических наук, начальник кафедры исполнения наказаний,
Санкт-Петербургский университет
Федеральной службы исполнения наказаний Российской Федерации

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ НА СОВРЕМЕННОМ ЭТАПЕ ЕЕ РЕФОРМИРОВАНИЯ

Аннотация. В представленной научной статье предпринимается попытка комплексного рассмотрения современных направлений цифровой трансформации уголовно-исполнительной системы Российской Федерации. Каждое из основных направлений цифровой трансформации подвергается отдельному

анализу и изучению. Отдельно в научной статье обращено внимание на анализ действующих нормативных правовых и директивных документов в сфере цифровой трансформации и информатизации уголовно-исполнительной системы Российской Федерации.

Ключевые слова: право, цифровые технологии, цифровая трансформация, уголовно-исполнительная система, цифровизация, осужденный, цифровой профиль

DIGITAL TRANSFORMATION OF THE PENAL ENFORCEMENT SYSTEM OF THE RUSSIAN FEDERATION AT THE PRESENT STAGE OF ITS REFORM

Abstract. The article an attempt is made to comprehensively consider the modern directions of digital transformation of the penal system of the Russian Federation. Each of the main directions of digital transformation is subjected to a separate analysis and study. Separately, the scientific article draws attention to the analysis of existing regulatory legal and policy documents in the field of digital transformation and informatization of the penal system of the Russian Federation

Keywords: Law, Digital technologies, Digital transformation, Penal enforcement system, Digitalization, Convict, Digital profile

Введение. Стремительное развитие современного общества связано с процессами его информатизации и цифровизации. Данные актуальные направления в том числе обусловлены реализацией национального проекта «Цифровая экономика», принятого в 2019 г. Правительством Российской Федерации [4. С. 116].

В указанный национальный проект включаются отдельные федеральные проекты, планируемые к реализации и в том числе проекты, предусматривающие обеспечение информационной безопасности и цифровую трансформацию отдельных сфер жизнедеятельности в целом.

Несомненным является факт того, что в процессе реализации национального проекта в той или иной степени должны быть задействованы все государственные учреждения и органы, и в том числе правоохранительные. Данное умозаключение относится и к уголовно-исполнительной системе Российской Федерации.

Положения большинства государственных проектов Российской Федерации («Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг.», «Информационное общество» и др.), связанные с цифровизацией также относятся в части касающейся к деятельности уголовно-исполнительной системы РФ [8. С. 42].

Основная часть. Развитие уголовно-исполнительной системы РФ на современном этапе связано со многими вызовами, в том числе с необходимостью адаптации материально-технического обеспечения исправительных учреждений, а также в целом объектов УИС РФ к современным требованиям научно-технического прогресса, цифровых технологий, искусственного интеллекта и т. д.

В целом данный процесс адаптации затрагивает и такое направление развития УИС РФ как цифровая трансформация.

Процесс цифровой трансформации неоднозначно воспринимается в научной и учебной литературе. Цифровую трансформацию сравнивают с понятием «информатизации». Некоторые исследователи говорят о том, что термин «цифровая трансформация» является слишком широким, не отражающим реальных процессов развития указанной сфере общественных отношений [3. С. 23].

На сегодняшний день цифровая трансформация УИС РФ регламентируется рядом нормативных, а также директивных документов [4. С. 121].

Нормативные правовые акты в указанной сфере общественных отношений предусматривают следующие актуальные направления цифровой трансформации УИС РФ:

– внедрение информационной системы «Электронная очередь»;

– внедрение проекта «Цифровой профиль осужденного»;

– развитие информационно-технического обеспечения пожарной безопасности УИС РФ;

– обеспечение информационной безопасности УИС РФ;

– переход на отечественное программное обеспечение;

– обеспечение функционирования информационных систем, обеспечивающих учебный процесс в образовательных организациях ФСИН России и др.;

– сквозную автоматизацию рабочих процессов, формирование баз данных в сфере функционирования УИС РФ;

– внедрение технологий искусственного интеллекта;

– создание единого защищенного управляемого информационного пространства, обеспечение информационной безопасности УИС РФ;

– внедрение в деятельность учреждений УИС РФ различных электронных баз.

Необходимо отметить, что мероприятия по цифровой трансформации УИС РФ в вышеуказанных документах коррелируют между собой и во многом схожи и взаимодополняют друг друга.

Кратко остановимся на анализе некоторых из вышеперечисленных направлений цифровой трансформации УИС РФ.

Реализация проекта «Цифровой профиль осужденного» позволит накапливать и анализировать информацию различного характера об осужденном с помощью технологий искусственного интеллекта. В том числе цифровой профиль осужденного может быть использован при реализации правовых норм об установлении административного надзора за лицами, освобожденными из мест лишения свободы, а также в рамках предполагаемого введения в практику деятельности службы пробации в РФ. При составлении заявления в суд об установлении административного надзора сотруднику исправительного учреждения будут предлагаться наиболее оптимальные варианты административный ограничений, которые не будут противоречить или затруднять процесс ресоциализации осужденного в рамках программы ресоциализации, которая будет построена на основе работы искусственного интеллекта, анализирующего данные цифрового профиля осужденного. Также использование цифрового профиля осужденного в рамках административного надзора должно убрать излишнюю формальность в деятельности сотрудников органов внутренних дел [1. С. 108].

Развитие системы электронного документооборота в УИС РФ. С развитием информационных технологий движение документов внутри учреждений и органов УИС РФ стало прозрачным, что позволило улучшить качество контроля исполнительской дисциплины[6. С. 67]. На сегодняшний день система электронного документооборота успешно применяется во всех учреждениях и органах УИС РФ.

Развитие системы электронного документооборота УИС РФ на современном этапе предполагает дополнение ее новыми функциями и возможностями, позволяющими в том числе наиболее эффективно достигать целей контроля за исполнительской дисциплиной.

Обеспечение информационной безопасности УИС РФ является одним из приоритетных направлений ее цифровой трансформации.

Новым подходом в обеспечении информационной безопасности является применение методов проактивной защиты [7. С. 131].

Также важное направление цифровой трансформации УИС РФ составляет формирование цифровой культуры сотрудников ФСИН России [2. С. 200].

Заключение. Таким образом процессы цифровой трансформации на сегодняшний день присущи и уголовно-исполнительной системе РФ. Особо актуальными направлениями в сфере цифровой трансформации УИС РФ на наш взгляд являются следующие: внедрение в деятельность УИС РФ технологий искусственного интеллекта; развитие системы электронного документооборота в УИС РФ; обеспечение информационной безопасности УИС РФ; реализация проекта «Цифровой профиль осужденного»; формирование цифровой культуры сотрудников УИС РФ и др.

Список литературы

1. Буравов И. С. Использование цифрового профиля, осужденного в административном надзоре за лицами, освобожденными из мест лишения свободы // Актуальные вопросы российского права: сборник статей Всероссийской научно-практической конференции. Пенза, 2022. С. 108.

2. Дуров В. А., Антоновский А. В. К вопросу о формировании цифровой культуры сотрудников ФСИН России // Прикладная психология и педагогика. 2022. Т. 7, № 3. С. 200.

3. Зубарев С. М. Правовые риски цифровизации государственного управления // Актуальные проблемы российского права. 2020. № 6. С. 23.

4. Ковалев С. Д. Цели и стратегические задачи цифровой трансформации уголовно-исполнительной системы // Пенитенциарное право: юридическая теория и правоприменительная практика. 2022. № 1 (31). С. 121.

5. Ковалев С. Д. Цифровая трансформация новый этап в развитии ФСИН России // Вестник Томского института повышения квалификации работников ФСИН России. 2022. № 1 (11). С. 116.

6. Мурович Н. В., Новикова Ю. И. Контроль за исполнительской дисциплиной в уголовно-исполнительной системе Российской Федерации посредством системы электронного документооборота // Ведомости уголовно-исполнительной системы. 2019. № 12 (211). С. 66–69.

7. Пастухов П. С., Сурин Н. В. Информационная безопасность цифровизации органов государственной власти (на примере уголовно-исполнительной системы) // Вестник Пермского института ФСИН России. 2021. № 2 (41). С. 131.

8. Царькова Е. Г. К вопросу использования массовых открытых онлайн-курсов при профессиональной подготовке сотрудников УИС // Антропогогика. 2022. № 1 (5). С. 42.

Е. В. Горенская,
кандидат юридических наук, доцент,
Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации

АКТУАЛЬНЫЕ ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ АВТОМОБИЛЬНОГО ТРАНСПОРТА

Аннотация. В статье рассмотрены понятийно-содержательнее аспекты такого важного направления безопасности автомобильного транспорта как кибербезопасность. Определены пути совершенствования кибербезопасности автомобильного транспорта, в том числе внедрение цифровых технологий и беспилотных транспортных средств, построение Единой цифровой транспортно-логистической среды, а также использование онлайн-тахографов. Обоснован вывод о необходимости повышения уровня кибербезопасности автомобильного транспорта путем проведения мероприятий на государственном уровне.

Ключевые слова: автомобильный транспорт, автомобиль, безопасность, цифровые технологии, кибербезопасность, киберзащищенность, тахограф

CURRENT ISSUES OF CYBERSECURITY OF MOTOR TRANSPORT

Abstract. Discusses the conceptual and substantive aspects of such an important area of road transport security as cybersecurity. The ways of improving the cybersecurity of road transport, including the introduction of digital technologies and unmanned vehicles, the construction of a unified digital transport and logistics environment, as well as the use of online tachographs, have been identified. The conclusion about the need to increase the level of cybersecurity of road transport by holding events at the state level is substantiated.

Keywords: Automobile transport, Automobile, Security, Digital technologies, Cybersecurity, Cyber security, Tachograph

Автомобильный транспорт (АТ) – один из самых распространенных видов транспорта, образующих в совокупности транспортную систему Российской Федерации, отличающийся скоростью доставки и маневренностью, позволяющей изменить маршрут в случае возникновения форс-мажора, однако у него небольшая грузоподъемность и высокая себестоимость эксплуатации (с учетом цены на топливо). На сегодняшний день около 56 млн транспортных средств (ТС), в том числе

автомобильных транспортных средств (АТС), являются единицами автомобильного транспорта. Около миллиона из них задействовано в пассажирских перевозках (в основном, это автобусы, на которых перевозится 90 % пассажиров). И в данной ситуации остро встает вопрос обеспечения безопасности пассажирских перевозок, сохранности грузов и багажа, а также самих транспортных средств [15].

При этом с учетом современного развития концепции цифрового государства и цифровой правовой среды [12, 14] речь идет уже не просто об обеспечении безопасности [16], а кибербезопасности объектов автомобильного транспорта, к которым отнесены «объекты автотранспортного бизнеса, включая предприятия отрасли и занимаемые ими земельные участки с коммуникациями, производственные и вспомогательные здания и сооружения, технологическое и вспомогательное оборудование, нематериальные активы (транспортные и производственные технологии, нормативно-техническая документация, изобретения, ноу-хау и т. п.), объекты инфраструктуры предприятий и организаций автомобильного транспорта» (см. п. 2.5 Требований к исполнителю услуг по оценке автотранспортных средств и объектов отрасли автомобильного транспорта. РД-03112194–1039–99. Система «СЕРТОЦАТ»).

Возникает вопрос о содержании термина «кибербезопасность», который в настоящее время законодательно не закреплен. Специалисты предлагают понимать под кибербезопасностью «условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться не желательными» [5].

Таким образом, на наш взгляд, происходит увязка одного термина, который не имеет законодательного закрепления, с другим термином – «киберпространство», который упоминается в ряде нормативных правовых актов, однако его дефиниция в данных актах не приводится. Наиболее легитимными представляются понятия, приведенные в Международном стандарте ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity [4]. Специалисты также предлагают свои определения киберпространства, например, Д. Е. Добринская считает его «пространством функционирования продуктов информационно-коммуникационных технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения информации, обмена и управления ею, а также осуществления коммуникаций в условиях множества различных сетей» [9].

Если рассматривать кибербезопасность как направление безопасности автомобильного транспорта, то его можно рассматривать:

1) в широком смысле – как совокупность условий, при которых все части и элементы киберпространства (интернет-ресурсы, системы, серверы, средства управления и контроля, и др.), связанного с автомобильным транспортом (и в целом с транспортной системой России [11]), защищены от большинства (в идеале – от всех) как внешних, так внутренних, вызовов и угроз;

2) в узком смысле – как защиту определенного объекта автомобильного транспорта или автомобильного транспортного средства от любых инцидентов, от актов незаконного вмешательства, а также от преступных посягательств (здесь

речь идет о степени защиты системы управления объектом АТ или АТС, их оборудованности средствами активной (высокая устойчивость, отличная управляемость, надежные тормозные свойства) и пассивной (специальная конструкция кузова, ремни, подушки безопасности, голосовые информаторы [19] и др.) безопасности, многие из которых сейчас управляются дистанционно, в том числе через Интернет).

Одним из самых перспективных путей совершенствования безопасности автомобильного транспорта, в том числе ее киберсоставляющей, является построение Единой цифровой транспортно-логистической среды (ЕЦТЛС). По мнению А. Семенова – заместителя министра транспорта Российской Федерации, «ЕЦТЛС – это не просто множество цифровых платформ. Для быстрого и безопасного обмена актуальными, унифицированными и достоверными данными обо всех этапах перевозки в реальном режиме времени необходима именно единая доверенная среда, которой и является ЕЦТЛС… Сервисы цифровой платформы позволяют реализовать взаимодействие с партнерами – странами ЕАЭС, со всей мировой транспортной системой в режиме единого окна. Целями проекта являются повышение эффективности управления транспортным комплексом, его интеграция в мировую цифровую транспортную систему. Особое внимание при реализации проекта уделяется безопасности российской транспортной системы» [17].

Второй путь – повсеместное внедрение и применение цифровых систем мониторинга (СМ), контроля и поддержания работоспособного состояния водителя (например, такой как СМ «Антисон», разработанной российской компанией XOR Group).

Министр транспорта Российской Федерации В. Савельев назвал внедрение цифровых технологий и беспилотных транспортных средств «одним из приоритетов в развитии транспортной отрасли» [10]. Так, Минтрансом России прорабатывается вопрос повсеместного использования онлайн-тахографов, фиксирующих нарушение максимальной скорости для конкретного ТС [2, 3]. Так, в настоящее время реализуется пилотный проект по сбору, хранению, обработке и передаче информации из тахографов, в рамках которого прорабатывается возможность осуществления передачи данных в АИС «Тахографический контроль» со всех устройств через тахограф.

Помимо этого, целесообразно повышать степень киберзащищенности автотранспортных средств, включая дистанционный контроль за системой торможения [19] и рулевого управления движущихся автомобилей (учитывая, что автомобили становятся все более компьютеризованными, возрастает опасность использования данного факта в преступных целях, а взлом или перехват управления автомобилем могут иметь крайне серьезные последствия). Специалисты в России и за рубежом [18] включают в понятие киберзащищенности: устойчивость компьютерных систем автомобиля против кибервзлома (особенно управляемых через беспроводное подключение (Wi-Fi- и bluetooth-модули), например, подсистем, связанных с управлением тормозами), установку в автомобилях самописцев, регулярное обновление программного обеспечения и аппаратных устройств, внедрение принципов сегментированности электронных систем автомобиля.

В данном случае необходимо отметить, что автомобили, которые имеют высокую степень компьютеризации, часто подвержены «IT-угонам» [7]. Соответственно,

любой объект АТ, например автопарк, может подвергнуться такой кибератаке. Так, в декабре 2020 г. сотрудниками УУР ГУ МВД России по Свердловской области совместно с ОУР УМВД России по г. Екатеринбургу была пресечена деятельность организованной группы, похищавших корейские и японские легковые машины (возбуждено уголовное дело по ч. 4 ст. 158 УК РФ). Преступники вносили изменения в программы контроллеров ЭСУД (электронная система управления двигателем), после чего устанавливали их в автомобили, а для того, чтобы открыть машины с сигнализацией использовали устройства для тестирования автосигнализаций (так называемые код-грабберы), а также радиотехническое оборудование для считывания радиосигналов (беспроводной ретранслятор ключа). Примечательно, что 20 лет назад о таких технических достижениях писали фантасты, а автовладельцы ставили противоугонки типа «Саргис» или «Полкан», фиксировали руль, клали на заднее сиденье милицейскую фуражку и т. п. [8]. На наш взгляд, в данном случае необходимо на основе обобщения практики противодействия IT-угонам обращать особое внимание на признаки возможной преступной деятельности, связанной с оборотом цифровой информации относительно автотранспортных средств [6].

Таким образом, приветствуя технический прогресс, необходимо повышать уровень кибербезопасности автомобильного транспорта путем совершенствования правового регулирования (в том числе закрепления на законодательном уровне понятий и приоритетных направлений кибербезопасности), моделирования ситуаций, угрожающих кибербезопасности, механизмов реагирования и защиты, в том числе уголовно-правовых и административных [13], а также эффективного выполнения мероприятий, предусмотренных Транспортной стратегией РФ [1].

Список литературы

1. О Транспортной стратегии Российской Федерации до 2030 года с прогнозом на период до 2035 года: распоряжение Правительства Российской Федерации от 27.11.2021 № 3363-р // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_402052/ (дата обращения: 19. 09.2022).

2. Об утверждении требований к тахографам, устанавливаемым на транспортные средства, категорий и видов транспортных средств, оснащаемых тахографами, правил использования, обслуживания и контроля работы тахографов, установленных на транспортные средств: Приказ Минтранса России от 13.02.2013 № 36 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_369096/ (дата обращения: 18.09.2022).

3. Об утверждении Порядка оснащения транспортных средств тахографами: Приказ Минтранса России от 21.08.2013 № 273 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_368231/ (дата обращения: 18.09.2022).

4. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. URL: https://www.iso.org/standard/44375.html (дата обращения: 18. 09.2022).

5. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5 (8). С. 39–42.

6. Бегишев И. Р., Бикеев И. И., Галимов А. Г. Признаки преступления в сфере обращения цифровой информации // Международный форум KAZAN DIGITAL WEEK – 2021. Казань, 2021. С. 261–268.

7. Горенская Е. В. Береги железного «коня» // Интерпол в России. 2000. № 4. С. 28–30.

8. Горенская Е. В. Проблемы борьбы с нелегальным автобизнесом. Москва: Московский институт МВД России, 2001. 179 с.

9. Добринская Д. Е. Киберпространство: территория современной жизни // Вестник Московского университета. 2018. Т. 24, № 1. С. 52–70.

10. Интервью Министра транспорта Виталия Савельева газете «Транспорт России». URL: https://mintrans.gov.ru/press-center/news/10012 (дата обращения: 18.09.2022).

11. Лещов Г. Ю. О контроле качества подготовки сил обеспечения транспортной безопасности: сборник материалов круглого стола / под общей ред. Т. А. Дикановой. 2019. С. 102–106.

12. Концепция цифрового государства и цифровой правовой среды: монография / Н. Н. Черногор, Д. А. Пашенцев, М. В. Залоило и др. Москва: ИЗиСП при Правительстве РФ: Норма: ИНФРА-М, 2021. 244 с.

13. Нудель С. Л. Уголовно-правовое воздействие в механизме обеспечения экономической безопасности (проблемы и тенденции законодательной регламентации) // Журнал российского права. 2020. № 6. С. 106–119.

14. Осипов Г. В., Хабриева Т. Я. Цифровизация: социология и право, концепция и практика социализации // Экономические стратегии. 2022. Т. 24, № 1 (181). С. 6–19.

15. Транспортная безопасность и противодействие терроризму на транспорте: правовые и организационные аспекты: сборник научных трудов по результатам II Международного научного форума / отв. ред. В. М. Корякин, Нестеров Е. А. Москва: Российский университет транспорта, Юридический институт, 2021. 286 с.

16. Трансформация правовой реальности в цифровую эпоху: сборник научных трудов / под общ. ред. Д. А. Пашенцева, М. В. Залоило. Москва: ИЗиСП при Правительстве РФ: ИНФРА-М, 2019. 213 с.

17. Цифровая эра – реальность. Алексей Семенов рассказал о цифровизации транспортной отрасли. URL: https://mintrans.gov.ru/press-center/interviews/508 (дата обращения: 18.09.2022).

18. Bokovnya A. Yu., Begishev I. R., Bikeev I. I., Almuhamedova I. R., Bersei D. D., Nechaeva N. B. Analysis of Russian judicial practice in cases of information security // International Journal of Engineering Research and Technology. 2020. Т. 13, № 12. С. 4602–4605.

19. Belova T. I., Torikov V. E., Titenok A. V., Shirobokova O. E., Starchenko E. V. Increasing the safety of the vehicle driver using the braking distance detectors // Natural Volatiles and Essential Oils. 2021. Т. 8, № 4. С. 7830–7839.

20. Kobrina N., Makoveckiy A., Makarenko D. Improving vehicle safety through the use of arduino controller-based automotive voice informants // Lecture Notes in Networks and Systems. 2021. Т. 188. С. 68–80.

Д. В. Грибанова,
юрист,
Аналитический центр уголовного права и криминологии,
магистр юридических наук

НЕКОТОРЫЕ ПРОБЛЕМЫ КВАЛИФИКАЦИИ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЯ) ПРЕСТУПНЫХ ДОХОДОВ

Аннотация. Настоящая статья посвящена актуальным проблемам квалификации легализации (отмывания) преступных доходов. В статье анализируются вопросы, связанные с обналичиванием денежных средств, виртуальными активами, проблемами квалификации отмывания, в случае его совершения на транснациональном уровне, а также вопросы, связанные с необходимостью разграничения предикатного и предикативного преступления.

Ключевые слова: легализация, отмывание, юрисдикция, виртуальные активы, квалификация, транснациональное преступление, предикатное преступление

ISSUES OF QUALIFICATION OF CRIMINAL MONEY LAUNDERING

Abstract. The article deals with the problems of qualification of criminal money laundering. The article examines the issues related to withdrawing funds, virtual assets, commission of money laundering at the transnational level, as well as the need to distinguish predicate and predicative crimes.

Keywords: Money laundering, Jurisdiction, Virtual assets, Qualification, Transnational crime, Predicate crime

Результатом трансформаций рыночных отношений, повлекших появление новых видов противоправной деятельности, в том числе сопряженных с проникновением в легальную экономику криминальных инвестиций, составляющих питательную среду для преступности, стало появление в Уголовном кодексе Российской Федерации новых составов преступлений, предусмотренных ст. 174, 174.1 УК РФ.

Небольшой опыт борьбы с отмыванием денег не позволяет РФ занять лидирующие позиции в этой сфере на международном уровне. По этой причине необходимо учитывать выработанные мировым сообществом стандарты противодействия легализации преступных доходов с целью усовершенствования «внутреннего» законодательства, в особенности таких организаций, как ООН, ФАТФ, БКБН и др.

В соответствии с Рекомендациями ФАТФ Российская Федерация стабильно проводит оценку рисков легализации с целью формирования на национальном уровне адекватного понимания рисков и угроз финансовой системе и экономике, а также принимает адекватные меры реагирования [2]. Тем не менее, как показывает анализ ФБД Росфинмониторинга, сохраняется достаточно высокая доля теневой экономики [5]. В 2021 г. организованные формы незаконного бизнеса по оказанию финансовых услуг и профессиональному отмыванию (так называемые теневые площадки, ландроматы) продолжали оставаться востребованным инструментом для функционирования теневой экономики, снабжения ее неконтролируемой наличностью и обеспечения

международных трансфертов в обход государственного контроля [5]. Одновременно с развитием компьютерных технологий, банковских систем, виртуальных валют, включением в экономику иностранных банков, увеличиваются возможности по совершению преступлений, предусмотренных ст. 174, 174.1 УК РФ.

Из всех видов преступной деятельности, легализация преступных доходов является максимально латентной, что подтверждается данным статистики. Так, согласно данным МВД по преступлениям экономической направленности в 2018 г. было выявлено 973 преступления, предусмотренных ст. 174, 174.1 УК РФ, что на 304 больше, чем за 2017 г. [6]. Предварительно расследовано было лишь 689 преступлений, из которых количество выявленных лиц, уголовные дела о которых были направлены в суд, составило только 569 [6]. Между тем, по данным Судебного департамента Верховного Суда Российской Федерации, за 1 полугодие 2018 г. по ст. 174, 174. 1 УК РФ было осуждено 16 человек[7].

В 2019 г. было выявлено 946 преступлений, предусмотренных ст. 174, 174.1 УК РФ [8], по данным составам было осуждено 12 человек соответственно [9]. В 2020 г. зарегистрировано 950 случаев отмывания преступных доходов [10], осуждено 17 человек [11]. В 2021 г. указанные показатели составили 949 [12] и 25 [13] соответственно.

Несмотря на то, что статистика свидетельствует об активизации борьбы с легализацией преступных доходов, изучение практики применения норм Уголовного Кодекса свидетельствует о неспособности государственных органов вовремя пресекать преступления, предусмотренные ст. 174, 174.1 УК РФ, и эффективно их расследовать. Вследствие отсутствия единства мнений в науке и практике правоохранительные органы принимают противоположные решения в схожих ситуациях. Страдает и доказательственная база, которая не всякий раз исчерпывающе демонстрирует связь между легализуемыми имущественными ценностями и исходным преступлением, доказывает наличие цели, отличающей данный состав от иных экономических преступлений[20].

Остановимся на некоторых наиболее актуальных теоретических и практических проблемах, связанных с легализацией преступных доходов (отмыванием).

1. **Проблема соотношения «обналичивания» и легализации преступных доходов. Вопросы квалификации.** В настоящее время проблема обналичивания в РФ является остроактуальной. Так, например, «веерное» обналичивание стало самой популярной схемой отмывания в 2021 г. По данным ЦБ, объем незаконно обналиченных средств в первом полугодии 2021 г. составил 17,5 млрд руб. [24].

В доктрине можно встретить позицию, согласно которой совершение легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем, возможно лишь путем введения этого имущества в легальный оборот. Аргументируется это тем, что только в таком случае будет поражаться непосредственный объект преступления – легальный оборот [21]. В свою очередь, незаконное обналичивание денежных средств подразумевает получение наличных денежных средств, не отраженных в бухгалтерских документах.

Вместе с тем, согласно Постановлению Пленума Верховного Суда РФ от 7 июля 2015 г. № 32, цель придания правомерного вида владению, пользованию

и распоряжению денежными средствами или иным имуществом, приобретенными преступным путем может быть установлена на основании совершения финансовых операций или сделок по обналичиванию денежных средств [21], т. е. посредством их вывода из легального экономического оборота.

Вопреки мнению исследователей, утверждающих, что «обналичивание» не поражает объект преступления, предусмотренный ст. 174, 174.1 УК РФ, с этим сложно согласиться. Во-первых, документальный след движения денежных средств в результате «обналичивания» прерывается по каналам банковской системы, что позволяет придать анонимный характер капиталу, и охватывается понятием «сокрытие». Во-вторых, по сути, это тот же фиктивный документооборот (та же задокументированная мнимая сделка). В-третьих, легализация преступных доходов и обналичивание – составляющие одного процесса, а именно перемещения денежных средств между теневой и легальной экономиками.

Данный вывод подтверждается судебной практикой. Так. в одном из приговоров отмечается, что перевод денежных средств, полученных преступным путем, на банковские карты, открытые на имя виновного, и их дальнейшее обналичивание были выполнены лицом в целях конспирации и в целях придания правомерного вида их получения, а в последующем владения, пользования и распоряжения [16].

Кроме того, как показывает практика, рост «обналичивания» в экономике увеличивает комиссию за совершения данной операции [18]. Зарубежный опыт также подтверждает, что сокращение безналичной массы при одновременном увеличении наличной значительно сказывается на устойчивости финансовой системы в целом, а значит, должен быть разработан механизм, основанный на их оптимальном сочетании [17].

Вместе с тем необходимо сделать оговорку – в свете рассматриваемого вопроса мы не говорим о полном отождествлении процессов обналичивания и отмывания. С позиции права верным это будет только тогда, когда обналичивание денег является способом их отмывания, т. е. когда посредством данного перемещения имеет место утаивание или искажение природы происхождения, движения и действительной принадлежности денежных средств.

2. **Виртуальные активы (криптовалюта) и легализация преступных доходов.** Постановление Пленума Верховного Суда РФ от 26.02.2019 № 1, исходя из положений ст. 1 Конвенции Совета Европы об отмывании от 16 мая 2005 года и с учетом Рекомендации 15 ФАТФ, предметом легализации преступных доходов признало в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления [4]. На этой основе некоторыми авторами принимается в качестве аксиомы в силу кажущейся очевидности то, что предметом ст. 174, 174.1 УК РФ являются виртуальные активы (криптовалюта), которые, следовательно, включаются в гражданско-правовое понятие «иное имущество», с чем мы не можем согласиться [19].

Внимательное изучение текста Постановления Пленума Верховного Суда РФ позволяет говорить о том, что виртуальные активы, помещенные в описание предмета преступления, на самом деле являются лишь источником, из которых данный предмет преобразуется, на что нам прямо указывают высший судебный орган и судебная практика [14].

Например, в приговоре суд установил, что Х. с целью сокрытия преступного источника дохода и маскировки легализуемого имущества с преступным источником его происхождения, совершал финансовые операции, а именно «выводил полученные денежные средства, преобразованные из виртуальных активов (криптовалюты) через счета «обменники» [15].

Не затрагивая проблемы сущности криптовалюты как объекта права применительно к легализации, отметим, что на данный момент дискуссий, пожалуй, не вызывает, то, что, во-первых, криптовалюта – это как минимум ценный экономический актив. Лица готовы принимать их в оплату товаров, работ и услуг, обмениваться ими. Основной акцент делается на субъективном отношении участников оборота, наличие у них имущественного интереса. Во-вторых, что право признает имущественный интерес в виде презумпции. При этом криптовалюта передается от лица к лицу «навсегда» – соответственно право, как таковое, не может вернуться.

Несмотря на то, что подобные рассуждения не имеют под собой практического обоснования, поскольку, как указывалось выше, de lege lata предметом легализации являются именно денежные средства, полагаем, что признание виртуальной валюты объектом права сомнительно ввиду невозможности принудительного исполнения обязательства сторонами по сделке, на что неоднократно указывал Росфинмониторинг. А что это за право, которое нельзя исполнить?

3. **Связь предикатного преступления и легализации преступных доходов на транснациональном уровне.** Рассмотрим две возможные ситуации. Первая – когда соответствующее предикатное преступление, подпадающее под юрисдикцию иностранного государства, является преступлением по уголовному праву РФ. Вторая ситуация – когда предикатное преступление (рассматриваемое с точки зрения российского уголовного права) в другом государстве либо не является уголовно наказуемым, либо не рассматривается как предикатное для отмывания преступных доходов.

Если в отношении первого примера никаких вопросов не возникает, поскольку предикатное преступление признается именно преступлением, а не правонарушением, то в отношении второго примера, как нам кажется, требуется системный подход к анализу действующих уголовно-правовых норм.

Так, уголовный закон характеризует источник отмываемых доходов не как «незаконный», а как «преступный», при этом преступный характер приобретения имущества должен устанавливаться на основании документов, перечисленных в п. 4 Постановления Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 32 г. Учитывая, что легализация преступных доходов является все-таки вторичной преступной деятельностью, исходя из смысла ч. 2 ст. 140 УПК возникает необходимость доказывать факт совершения первичного преступления. Признавать действия лица направленными на отмывание доходов, полученных преступным путем, может только суд на основании рекомендаций Постановления Пленума ВС РФ.

Согласно ст. 8 УК РФ, основанием уголовной ответственности является совершение деяния, содержащего все признаки состава преступления. При этом не уточняется, что включает в себя понятие «деяние». Учитывая, что легализация преступных доходов не может рассматриваться автономно от предикатного преступления, значит, в данном случае «деяние» подразумевает как предикатное

преступление, так и предикативное, которые должны содержать признаки состава преступления, предусмотренного настоящим Уголовным Кодексом.

Решение данного вопроса выводится на основе системного толкования норм материального и процессуального права. Данный вывод не противоречит пониманию положений международных документов, а именно подп. «с» п. 2 ст. 6 Палермской Конвенции[1], а также Рекомендации 1 ФАТФ[3], допускающих такой узкий подход. Другими словами, привлечение к уголовной ответственности на территории РФ будет возможным лишь в случае признания основного посягательства «преступлением» российским уголовным законом. Иное бы, к противоречило принципу законности, закрепленного в ст. 3 УК РФ, поскольку объективно-противоправный характер основного преступления попросту не обнаруживался бы ввиду отсутствия надлежащей статьи УК РФ.

4. **Разграничение основного (предикатного) преступления от легализации преступных доходов.** Слияние «сделки» по отмыванию денег и лежащего в ее основе предикатного преступления на практике вызывает значительные сложности, в особенности в случаях совершения мошенничества, выступающим основным преступлением. Необходимо помнить, что отмыванию предшествует предикатное преступление, которое на момент легализации должно считаться оконченным (или прерванным по независящим обстоятельствам). В таком случае проблем с практикой применения нормы об ответственности за легализацию не возникает.

На необходимость разграничения предикатного и предикативного преступления особое внимание обращается и в зарубежной практике. Для этого хотелось бы обратиться к опыту США ввиду определенного сходства антиотмывочного регулирования. Так, например, в деле United States v. Butler, 211 F. 3d 826, 830 (4th Cir. 2000) [22] отмечалось, что отмывание не может происходить по той же самой сделке, в результате которой эти средства впервые становятся преступно приобретенными. В деле United States v. Johnson, 971 F.2d 562 (10th Cir. 1992) [23] лицо обманным путем вынудило потерпевшего перевести денежные средства непосредственно на его счет. Суд пришел к выводу, что такая передача не является отмыванием денег, потому что средства были стали получены преступным путем только в момент передачи.

Вместе с тем возникает вопрос: может ли быть совершена легализация преступных доходов, если предикатное преступление еще не окончено (момент юридического, а не фактического окончания)? Весьма показательным будет являться пример, когда лицо предварительно получает вознаграждение за участие в предикатном преступлении, совершает легализацию данной суммы, и только впоследствии совершает предикатное преступление. Основной вопрос, который тут может возникнуть, – считаются ли данные денежные средства имуществом, полученными лицом в результате совершения преступления?

Если разбить данный пример на несколько эпизодов, то на момент принятия денежных средств действия лица можно было бы квалифицировать как приготовление (но в силу ч. 2 ст. 30 уголовная ответственность будет наступать за приготовление к тяжкому и особо тяжкому преступлению). Далее, если лицо отмывает денежные средства, полученные им «заранее» за совершение основного преступления, которое во временном поле лежит за рамками легализации, представляется вполне приме-

нимой юридическая конструкция «фикции» – чтобы денежные средства обладали признаком полученных «в результате совершения преступления», будем считать их полученными якобы после совершения предикатного преступления, хотя фактически они, конечно же, имелись у лица и до его начала.

Что делать в случае, если лицо принимает эти денежные средства, их легализует, но отказывается от совершения предикатного преступления? В данном случае, наиболее ярко, как нам кажется, проявляется различие между формулировками «приобретенные преступным путем» и «приобретенные лицом в результате совершения им преступления». Однако поскольку в силу положений действующего уголовного закона требуется получение денежных средств или иного имущества именно в результате совершения преступления, такое лицо невозможно будет привлечь к уголовной ответственности как за «самоотмывание», так и за «легализацию имущества, приобретенных другими лицами преступным путем», поскольку иные лица в приведенном примере отсутствуют.

Таким образом, отметим, что разработка и согласование спорных моментов сыграют роль своеобразного звена между правоприменительной деятельностью и законом, особенно в условиях повышенной общественной опасности легализации преступных доходов и его транснациональном характере. Из всего вышесказанного можно заключить следующее:

– «обналичивание» посягает на объект преступления, предусмотренный ст. ст. 174, 174.1 УК РФ, в случае, когда является способом отмывания, т. е. когда посредством перемещения денежных средств имеет место утаивание или искажение их природы, происхождения, движения и действительной принадлежности;

– виртуальные активы (криптовалюта) не являются не предметом легализации; это источник, из которых преобразуются денежные средства, на что нам прямо указывает высший судебный орган и судебная практика;

– если предикатное преступление (рассматриваемое с точки зрения российского уголовного закона) в другом государстве либо не является уголовно наказуемым, либо не рассматривается в качестве предикатного для отмывания преступных доходов, привлечение к уголовной ответственности на территории РФ будет возможным лишь в случае признания основного посягательства «преступлением» российским уголовным законом;

– легализация преступных доходов может иметь место и в том случае, когда предикатное преступление еще окончено, например, в случае, когда лицо предварительно получает вознаграждение за участие в основном преступлении, совершает легализацию данной суммы, и только впоследствии его совершает преступление. При этом, несмотря на то, что лицо отмывает денежные средства, полученные им «заранее» за совершение основного преступления, которое во временном поле лежит за рамками легализации, представляется вполне применимой конструкция юридической фикции.

Список литературы

1. Конвенция против транснациональной организованной преступности (15 ноября 2000 года). URL: http://www.fedsfm.ru/documents/international-conventions

2. Рекомендации ФАТФ. Пленарное заседание. Февраль 2012 года. The FATF recommendations // adopted by the FATF plenary in February 2012/Updated October 2018. International standards on combating money laundering. URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

3. Рекомендации ФАТФ. URL: http://org-rsa.ru/upload/Pril_4.pdf

4. Постановление Пленума Верховного Суда РФ от 26.02.2019 № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // Бюллетень Верховного Суда РФ. 2019. № 4, апрель.

5. Публичный годовой отчет о деятельности Росфинмониторинга, 2021 г. URL: https://www.fedsfm.ru/content/files/documents/2022/annualreport21.pdf

6. Краткая характеристика состояния преступности в Российской Федерации за январь – ноябрь 2018 года. URL: https://мвд.рф/reports/item/15304733/

7. Сводные статистические сведения о состоянии судимости в России за 1 полугодие 2018 года. URL: http://www.cdep.ru/index.php?id=79&item=4759

8. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2019 года. URL: https://мвд.рф/reports/item/19412450/

9. Сводные статистические сведения о состоянии судимости в России за 1 полугодие 2019 года http://www.cdep.ru/index.php?id=79&item=4759

10. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2020 года. URL: https://мвд.рф/reports/item/22678184/

11. Сводные статистические сведения о состоянии судимости в России за 2020 год. URL: http://www.cdep.ru/index.php?id=79&item=5669

12. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2021 года. URL: https://мвд.рф/reports/item/28021552/

13. Сводные статистические сведения о состоянии судимости в России за 2021 год. URL: http://www.cdep.ru/index.php?id=79&item=6121

14. Приговор № 1–259/2019 от 17 июля 2019 г. по делу № 1–259/2019. Новотроицкий городской суд (Оренбургская область).

15. Приговор № 1–268/2019 от 5 июля 2019 г. по делу № 1–268/2019. Златоустовский городской суд (Челябинская область).

16. Приговор № 1–171/2018 от 25 мая 2018 г. по делу № 1–171/2018 Курчатовский районный суд г. Челябинска (Челябинская область).

17. Бердышев А. В. Зарубежный и Российский опыт сокращения наличных платежей в экономике // Вестник ГУУ. 2019. № 4.

18. Дульская Е. Г. Использование специальных знаний для выявления незаконного обналичивания денежных средств как способа вывода активов // Вестник Университета имени О. Е. Кутафина. 2018. № 7.

19. Коренная А. А., Тыдыкова Н. В. Криптовалюта как предмет и средство совершения преступлений // Всероссийский криминологический журнал. 2019. № 3.

20. Крачун Ю. В. Совершенствование методики расследования преступлений, связанных с легализацией (отмыванием) денежных средств и иного имущества,

полученных преступным путем: дис. … канд. юрид. наук. Рост. юрид. ин-т МВД РФ. Ростов-на-Дону, 2016. С. 266.

21. Якимов О. Ю. Легализация доходов, приобретенных преступным путем / под науч. ред. Н. А. Лопашенко. Санкт-Петербург: Юрид. центр Пресс, 2005.

22. United States v. Butler, 211 F. 3d 826, 830 (4th Cir. 2000).

23. United States v. Johnson, 971 F.2d 562 (10th Cir. 1992).

24. «Веерное» обналичивание стало самой популярной схемой отмывания в 2021 году. URL: https://rg.ru/2021/10/07/veernoe-obnalichivanie-stalo-samoj-populiarnoj-shemoj-otmyvaniia-v-2021-godu.html

Н. П. Громовенко,
старший преподаватель
кафедры гражданского и уголовного права и процесса,
Сочинский государственный университет

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ УЧЕТЕ ОБСТОЯТЕЛЬСТВ, СМЯГЧАЮЩИХ УГОЛОВНОЕ НАКАЗАНИЕ

Аннотация. Трансформационные информационные процессы развития общества и права обозначили новый виток модернизации одной из фундаментальных наук – уголовного права. Автор обсуждает основные проблемы публично-правовой сферы уголовного права, моделирует направления, перспективы внедрения технологии искусственного интеллекта, на примере установления факта аморального поведения потерпевшего и преступления, указывая на противоречия российского законодательства и возможности использования рискориентированного подхода, сопоставления и моделирования ситуации в целях одного из путей формирования машиночитаемого уголовного права.

Ключевые слова: уголовное наказание, обстоятельства, смягчающие уголовное наказание, электронное уголовное дело, искусственный интеллект, цифровая информация, рискориентированный подход

ON THE USE OF ARTIFICIAL INTELLIGENCE TEHNOLOGY TAKING INTO ACCOUNT THE CIRCUMSTANCES MITIGATING CRIMINAL PUNISHMENT

Abstract. Transformational information processes in the development of society and law have marked a new round of modernization, one of the fundamental sciences – criminal law. The author discusses the main problems of the public-legal sphere of criminal law, models the directions and prospects for the introduction of artificial intelligence technology by the example of establishing the fact of immoral behavior of the victim and the crime, pointing to the contradictions of Russian legislation and the possibility of using a risk-based approach, comparing and modeling the situation for the purpose of one of the ways of forming machine-readable criminal law.

Keywords: Criminal punishment, Circumstances mitigating criminal punishment, Electronic criminal case, Artificial intelligence, Digital information, Risk-oriented approach

Современное измерение российского права в течение последних лет характеризуется новыми стандартами развития, опосредованными в цифровых технологических подходах, проникающих в различные отрасли, в том числе и в уголовное право.

Цифровые технологии XXI в. постепенно проходят эквивалент потенциальной необходимости в жизнедеятельности общества. Традиционное осмысление базовых институтов уголовного права дополняется моделями переориентирования и внедрения в формат машиночитаемого уголовного права.

Технологии искусственного интеллекта, способного алгоритмизировать правовое пространство воспринимаются сегодня как некое новое явление, сформулируемое одной из национальных задач со стороны государства [2].

Научное сообщество разносторонне подходит к использованию нейросетей и формированию искусственного интеллекта в уголовно-правовом измерении.

Н. Д. Оранжиреев отмечал, что «ввиду отсутствия единообразного способа учета обстоятельств дела процесс назначения наказания сильно напоминает гадание на кофейной гуще. Необходимо установить строгие математические количественные эквиваленты для всех преступлений, выразив их в соответствующих санкциях, а для различных обстоятельств, существенных с точки зрения определения виновности осужденного, предусмотреть специальные коэффициенты, например, при соучастии коэффициент исполнителя составит 1,0; подстрекателя –0,9; пособника – 0,75 и т. д. Окончательное наказание необходимо определять путем алгебраических операций с эквивалентом преступления и индивидуальными коэффициентами» [9. С. 250]. Н. Кристи и вовсе предлагает не только применять строго формализованную систему назначения наказания, но и устранить человека из данного процесса, передав все функции назначения наказания ЭВМ [8. С. 176].

Отдельными современными учеными [10. С. 56] видится применение данной новации в общей теории уголовного права, и только в качестве помощника в раскрытии преступлений, использовании интеллектуальных возможностей цифровых технологий в документообороте.

Любопытным видится формирование идеи расширения обстоятельств, отягчающих преступное деяние [7. С. 33], предусмотренных ст. 63 УК РФ, по фактам причастия к ним искусственного интеллекта, как некого субъекта, способствующего своими технологическими возможностями увеличить вероятность достижения желаемого результата, доказывая при этом, что это явление, сегодня не может быть воспринято как соучастие в преступлении, но, если внести поправки в уголовное законодательство, и использовать его как квалифицирующий признак, признав тем самым его в гл. 28 УК РФ, то интеллект может отчасти обладать уголовной правосубъектностью.

В одной из работ нами отстаивалась идея частичного применения искусственного интеллекта при учете обстоятельств, смягчающих уголовное наказание [6. С. 46–48], при этом указывалось: «…участие информационно-коммуникационных технологий (ИКТ), и как следствие искусственного интеллекта, в работе следователей принесет положительный эффект, помогая при этом сформировать

четко информационно выверенную характеристику личности подсудимого, что заложено в основу отдельных нормативных актов» [1].

Продолжая анализировать потенциальное применение цифровых технологий в системе мер, оказывающих влияние на обстоятельства, смягчающие уголовное наказание, следует обратить внимание на потенциальную возможность применения искусственного интеллекта в делопроизводстве по установлению факта аморального поведения потерпевшего и преступления, что предусмотрено п. «з» ч. 1 ст. 61 УК РФ.

Исходя из особенностей данного обстоятельства, следует отметить, что сегодня аморальность не всегда приветствуется судами, как обстоятельство, которое потенциально влечет к смягчению наказания. Материалы судебной практики достаточно скудно рассматривают его особенности [3]. Рассматривая мотивировочную часть обвинительного приговора, исходя из контекста нашего исследования, аморальность может быть приобщена, только по усмотрению суда, как смягчающее обстоятельство.

При этом, исходя из отдельной судебной практики [4], данное обстоятельство может не входить в описательную часть, не являясь при этом законом установленной документальной необходимостью объяснения причин судейского усмотрения. В тоже время, исходя из иных судебных материалов [5], судами может использоваться аморальность поведения потерпевшего как повод для преступления, при учете определения размера компенсации морального вреда. Именно с помощью применения искусственного интеллекта в судопроизводстве, эта коллизия может быть устранена, с установлением технологии машиночитаемого уголовного права.

Рассматривая этот вид обстоятельств мы тесным образом сталкиваемся с мотивационным поступком лица, совершившего деяние, его поведенческим характером, а, следовательно, в этом виде обстоятельств, по внешним критериям личности преступника, используя цифровые аутентификационные и идентификационные характеристики, необходима законодательная регламентация всесторонней оценка поведения преступника.

Полагаем, что необходимо проведение организационно-правовых процедур по подготовке специалистов правоохранительных органов в сфере использования новых цифровых технологий в работе с квалификацией составов преступлений, учитывающих один из немаловажных критериев, как смягчающие обстоятельства преступного деяния, предусмотренные ст. 61 УК РФ.

Так или иначе, система построения нового цифрового уголовно-правового пространства, с использованием технологий искусственного интеллекта, это задача, которая вписывается в стратегический контент российской правовой действительности будущего десятилетия, и тем не менее активные разработки, с учетом использования личностных характеристики преступника, имеют место быть.

Не отраженные в достаточной мере в современном праве, нормы, затрагивающие, аморальное поведение потерпевшего и преступление, установленные п. «з» части 1 статьи 61 УК РФ, уже закладывают основу необходимости изначального пересмотра и введения в правовой оборот в должном формате, путем внесения изменений в отдельные законодательные акты, и, лишь потом формирование на этой основе машиночитаемой нормы уголовного права.

Рассмотрев потенциальную возможность использования искусственного интеллекта в квалификации состава преступлений с учетом обстоятельств, смягчающих

наказание, необходимо отметить, что при любых обстоятельствах первичен риск систем искусственного интеллекта, поэтому требуется применение междисциплинарного подхода по применению данной технологии в уголовном праве.

Обращая внимание на обстоятельства, смягчающие наказание предстоит задача в разработке модели минимизации уголовно-правового риска, поскольку рассматриваемый нами контент во взаимосвязи с конституционными положениями (ст. 2, ч. 3 ст. 17, ст. 19, ч. 3 ст. 55) указывает на гарантированность и потенциальную возможность введения только тех ограничений, которые в демократическом правовом государстве необходимы для защиты конституционных ценностей, главной из которых являются права человека, с соблюдением критериев соразмерности баланса интересов государства и личности.

Именно подход рискориентированного взаимодействия, сопоставления и моделирования ситуации может послужить основой формирования модернизационных начал машиночитаемого уголовного права, где цифровые технологии вкупе с действующими уголовно-правовыми нормами сформируют новый подход в поставленной проблематике.

Список литературы

1. Федеральный закон от 27.12.2019 № 487-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам государственного единого статистического учета данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре» // Собрание законодательства РФ. 2019. № 52 (часть I). Ст. 7805.

2. Указ Президента РФ от 07.05.2018 № 204 (ред. от 21.07.2020) «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Собрание законодательства РФ. 2018. № 20. Ст. 2817; 2020. № 30. Ст. 4884.

3. Постановление Пленума Верховного Суда РФ от 22 декабря 2015 г. № 58 г. Москва «О практике назначения судами Российской Федерации уголовного наказания» // Бюллетень Верховного Суда РФ. 2016. № 2.

4. Постановление Пленума Верховного Суда РФ от 29.11.2016 № 55 «О судебном приговоре» // Бюллетень Верховного Суда РФ. 2017. № 1.

5. Постановление Пленума Верховного Суда РФ от 13.10.2020 № 23 «О практике рассмотрения судами гражданского иска по уголовному делу» // Бюллетень Верховного Суда РФ. 2020. № 12.

6. Громовенко Н. П. Цифровой формат мер, направленных на оптимизацию мер, направленных на оптимизацию учета обстоятельств, смягчающих уголовное наказание // Российский следователь. 2022. № 8. С. 46–48.

7. Капитонова Е. А. Искусственный интеллект как потенциальный носитель правового модуса личности: проблемы и перспективы // Наука. Общество. Государство. 2019. № 4 (28). С. 33.

8. Кристи Н. Пределы наказания. Москва: Прогресс, 1985. 176 с.

9. Оранжиреев Н. Д. Преступление и наказание в математической зависимости (идея и схема применения). Москва, 1916. С. 250.

10. Саргсян А. А. Перспективы цифровизации назначения и исполнения уголовного наказания // Пенитенциарная наука. 2022. № 2 (58). С. 56.

Е. И. Грузинская,
кандидат юридических наук, доцент,
Государственный морской университет имени Ф. Ф. Ушакова

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ КАК СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ МИРА И БЕЗОПАСНОСТИ ЧЕЛОВЕЧЕСТВА

Аннотация. В представленной статье обосновывается необходимость расширения квалифицированных составов деяний гл. 34 УК РФ «Преступления против мира и безопасности человечества» указанием на способ совершения преступления – использование цифровых технологий. При этом под цифровыми технологиями в отсутствие законодательного термина предлагается понимать уже известные национальному уголовному законодательству электронные, информационно-телекоммуникационные сети, включая сеть Интернет, а также сети связи общего пользования.

Ключевые слова: цифровые технологии, уголовный кодекс, преступления против мира и безопасности человечества, способ совершения преступления, квалифицированный признак

THE USE OF DIGITAL TECHNOLOGIES AS A WAY TO COMMIT CRIMES AGAINST THE PEACE AND SECURITY OF MANKIND

Abstract. The presented article substantiates the need to expand the qualified compositions of acts of Chapter 34 of the Criminal Code of the Russian Federation “Crimes against the peace and security of mankind” by indicating the method of committing a crime – the use of digital technologies. At the same time, in the absence of a legislative term, digital technologies are proposed to be understood as electronic, information and telecommunication networks already known to the national criminal legislation, including the Internet, as well as public communication networks.

Keywords: Digital technologies, Criminal code, Crimes against the peace and security of mankind, Method of committing a crime, Qualified attribute

В настоящее время мы живем в мире «цифры». Ей пронизана большая часть нашей жизни. «Цифра» обеспечивают доступность жизни. Посредством «цифры» осуществляется обмен информацией участниками различных правоотношений. Принято больше трех тысяч нормативно-правовых актов различной юридической силы, так или иначе регламентирующих отношения посредством «цифровых технологий». Однако при подобном расширенном их применении и растущем числе лиц, обладающих цифровыми навыками, следует отметить отсутствие законодательно закрепленного термина «цифровые технологии», имеет место лишь активное их упоминание в аспекте внедрения [12, 14], применения [11], совершенствования [16].

В ряде нормативных источников закреплено более узкое понятие «сквозная цифровая технология». Под последней понимается часть технологического процесса производства товаров, оказания услуг и выполнения работ, представляющая собой

совокупность процессов и методов поиска, сбора, хранения, обработки, предоставления и распространения информации, обеспечивающих в ходе хозяйственной деятельности по производству (поставке) товаров, оказанию услуг и выполнению работ: повышение результативности, точности или иных значимых характеристик технологического процесса; повышение качества или иных значимых характеристик производимых (поставляемых) товаров, оказываемых услуг и выполняемых работ (в том числе за счет сокращения брака) [10]. «Сквозными» цифровыми технологиями определены: искусственный интеллект; системы распределенного реестра; квантовые технологии; новые производственные технологии; компоненты робототехники и сенсорика; технологии беспроводной связи; технологии виртуальной и дополненной реальностей [13].

Обращение к доктринальным источникам позволяет констатировать отсутствие как единого подхода к определению цифровых технологий, так и использование различных терминов при исследовании их сущности – компьютерные технологии, цифровая коммуникационная технология, цифровая инфраструктура, информационные ресурсы, интернет-ресурсы, высокие технологии [1. С. 5–11; 5. С. 18; 6. С. 16–29; 8. С. 44–52; 18. С. 133–145]. В отраслевых научных источниках предпринимаются попытки сформулировать авторскую дефиницию. Так, под цифровыми технологиями в уголовном процессе, например, предлагается понимать определенную совокупность средств, приемов и методов собирания (поиска, обнаружения, фиксации, изъятия), обработки (в том числе с использованием искусственного интеллекта), передачи и представления информации о расследуемом событии для получения уголовно-процессуальных доказательств [17. С. 78].

Таким образом, можно предположить, что в обобщенном виде под цифровыми технологиями следует понимать определенный способ аккумулирования и распространения информации посредством использования электронных, информационно-телекоммуникационных сетей, включая сеть Интернет, а также сетей связи общего пользования.

Как было сказано выше, развитие цифровых технологий должно стать одним из ключевых факторов устойчивого развития общества. Как известно любое новое правомерное поведение рождает и его противоправную сторону. В связи с цифровизацией общества получают распространение и формы проявления преступного поведения с использованием цифровых технологий, что незамедлительно находит отражение в составах Особенной части УК РФ.

Наиболее часто в качестве криминообразующего или квалифицирующего признака объективной стороны преступления выступает способ совершения деяния. То есть именно та форма, в которой выразились общественно-опасные действия, те приемы и методы, которыми воспользовалось лицо для нарушения объекта уголовно-правовой охраны [4. С. 153–154]. Согласно толковому словарю, способ – это прием, действие, метод, применяемые при исполнении какой-нибудь работы, при осуществлении чего-нибудь [15. С. 439]. Поскольку преступление является одним из способов человеческой деятельности, под способом совершения преступления может пониматься совокупность приемов и методов, применяемых при осуществлении преступления.

В Уголовном кодексе Российской Федерации (далее – УК РФ) законодатель закрепил важное положение, согласно которому уголовный закон основывается на общепризнанных принципах и нормах международного права (ч. 2 ст. 2 УК РФ). В настоящее время действует более 100 международных документов, так или иначе связанных с охраной отношений, признаваемых объектами уголовно-правовой охраны.

В разд. XII УК РФ «Преступления против мира и безопасности человечества» нашли свое отражение соответствующие положения международных документов, направленных на регламентацию отношений, обеспечивающих достижение всеобщего уважения и соблюдения основных прав и свобод для всех, без различия расы, пола, языка и религии, выразившиеся в криминализации деяний, нарушающих нормы международного права – «Планирование, подготовка, развязывание или ведение агрессивной войны» (ст. 353 УК РФ); «Публичные призывы к развязыванию агрессивной войны» (ст. 354 УК РФ); «Реабилитация нацизма» (ст. 3541 УК РФ) «Разработка, производство, накопление, приобретение или сбыт оружия массового поражения» (ст. 355 УК РФ); «Применение запрещенных средств и методов ведения войны»; «Геноцид» (ст. 357); «Экоцид» (ст. 358 УК РФ); «Наемничество» (ст. 359 УК РФ); «Нападение на лиц и учреждения, которые пользуются международной защитой» (ст. 360 УК РФ), «Акт международного терроризма» (ст. 361 УК РФ).

Как правило, криминализация данных деяний во внутреннем законодательстве является результатом имплементации норм международного права в национальное уголовное законодательство. Не исключено, что процесс «одомашивания» [3. С. 12] международного уголовного права может приводить к тому, что отечественный законодатель с учетом изменений в общественной жизни, в том числе с ее цифровизацией, может расширить объективную сторону того или иного деяния, либо криминализировать ранее неизвестные Уголовному кодексу (в ряде случаев и менее изменяющимся международным нормам) способы преступного поведения. Последнее может относиться и к деяниям главы 34 УК РФ «Преступления против мира и безопасности человечества», объективная сторона которых весьма специфична.

С учетом реалий объективной действительности степень общественной опасности ряда деяний заключительной главы уголовного закона может повышаться именно благодаря использованию цифровых технологий.

Так, объективная сторона планирования агрессивной войны (ст. 353 УК РФ) предполагает действия, направленные на обеспечение разработки и выполнения планов (штабных мероприятий, концепции ведения основных боевых действий) начал и ведения войны: поиск союзников, аккумулирование необходимых денежных средств и материальных ресурсов, оплата военных заказов и т. д. [2. С. 24], т. е. совершения любого действия интеллектуального характера [9. С. 136]. Доказательством осуществления таких действий может служить наличие документально оформленных планов, процедур согласования военных действий, в том числе и на электронных носителях и размещенных в пространствах сети Интернет.

Публичные призывы к развязыванию агрессивной войны (ст. 354 УК РФ) подразумевают под собой устное, письменное или электронное обращение к неограниченному кругу лиц, психологическому воздействию на них, направленные на

формирование определенной общественной позиции. Здесь необходимо заметить, что в квалифицированном составе законодатель выделил в качестве объективного признака использование средств массовой информации, однако «цифровая» составляющая способа остается за рамками состава.

Объективная сторона того, что объединяется понятием «реабилитация нацизма» (ст. 3541 УК РФ), выражается в публичном, т. е. не имеющем частного характера (приватная беседа, личная переписка и т. п.) и совершенном в отношении определенно широкого (студенческая группа в аудитории) либо неопределенного (участники митинга, читатели печатных изданий, телезрители, пользователи Интернета) круга лиц: отрицании фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси; одобрении преступлений, установленных указанным приговором; распространении заведомо ложных сведений о деятельности СССР в годы Второй мировой войны; распространении заведомо ложных сведений о деятельности СССР в годы Второй мировой войны, о ветеранах Великой отечественной войны, сведений, о днях воинской славы и памятных датах России, связанных с защитой Отечества. Первые три разновидности деяния влекут более строгую ответственность, если они совершены (признаки альтернативны): лицом с использованием своего служебного положения; с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети Интернет [7. С. 496].

Как нам представляется объективная сторона наемничества, совершенная с помощью использования цифровых технологий, значительно облегчает его совершение. Вербовка, как одно из деяний состава преступления, предусмотренного ст. 359 УК РФ, означает деятельность, направленную на заключение соглашения с представителем третьего государства об участии в вооруженном конфликте за материальное вознаграждение. В данные действия входят поиск, приглашение людей для участия в вооруженном конфликте. Использование «цифры» значительно ускоряет и облегчает данный процесс.

Таким образом, можно прийти к выводу, что цифровизация общественных отношений привела и к значительному упрощению совершения противоправных деяний, что должно находить отражение и в криминализации общественно-вредного поведения. Учитывая крайнюю общественную опасность деяний главы 34 УК РФ, считаем целесообразным дополнить квалифицированные составы деяний, которые могут быть совершены, в том числе и посредством цифровых технологий, соответствующим указанием на данный способ.

Список литературы

1. Антонова Е. Г., Лавелина В. С. Цифровые технологии в правотворческой деятельности // Право и цифровая экономика. 2020. № 4. С. 5–11.

2. Арямов А. А. Преступления против мира и безопасности человечества: хрестоматийный курс лекций. Москва: Юрлитинфлрм, 2012. С. 24.

3. Богуш Г. И., Есаков Г. А., Русинова В. Н. Международные преступления: модель имплементации в российское уголовное законодательство: монография. Москва: Проспект, 2017. С. 12.

4. Велиев И. В. Об объективной стороне преступления: монография. Москва: ЮРКОМПАНИ, 2010. С. 153–154.

5. Высокотехнологическое право: генезис и перспективы: материалы III Международной межвузовской научно-практической конференции (Москва – Красноярск. 24–25 февраля 2022 г.) / Национальный исследовательский университет «Московский институт электронной техники»; Красноярский государственный аграрный университет. Красноярск, 2022. 346 с.

6. Гаджиев Х. И. Доктрина презумпции невиновности в век цифровых технологий // Журнал зарубежного законодательства и сравнительного правоведения. 2020. № 4. С. 16–29.

7. Егорова Н. А. Реабилитация нацизма: уголовно-правовой анализ // Криминологический журнал Байкальского государственного университета экономики и права. 2015. Т. 9, № 3. С. 496.

8. Жуков Д. В. Особенности защиты культурных прав в условиях развития цифровых технологий // Журнал российского права. 2020. № 9. С. 44–52.

9. Кибальник А. Г., Соломоненко И. Г. Преступления против мира и безопасности человечества / под науч. ред. докт. юрид. наук, проф. А. В. Наумова. Санкт-Петербург: Юридический центр Пресс, 2004. С. 136.

10. О государственной поддержке программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий (вместе с «Правилами предоставления субсидий из федерального бюджета на государственную поддержку программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий», «Положением о проведении конкурсного отбора на предоставление государственной поддержки программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий»): Постановление Правительства РФ от 03.05.2019 № 551 (ред. от 19.12.2019) // Собрание законодательства РФ. 2019. № 19. Ст. 2307.

11. О Национальном плане противодействия коррупции на 2021–2024 годы: Указ Президента РФ от 16.08.2021 № 478 // Собрание законодательства РФ. 2021. № 34. Ст. 6170.

12. Об утверждении Концепции подготовки кадров для транспортного комплекса до 2035 года: Распоряжение Правительства РФ от 06.02.2021 № 255-р // Собрание законодательства РФ. 2021. № 7. Ст. 1171.

13. Об утверждении методик расчета показателей федерального проекта «Цифровые технологии» национальной программы «Цифровая экономика Российской Федерации (вместе с «Методикой расчета показателя «Увеличение затрат на развитие «сквозных» цифровых технологий, процент», «Методикой расчета показателя «Увеличение объема выручки проектов (по разработке наукоемких решений, по продвижению продуктов и услуг по заказу бизнеса) на основе внедрения «сквозных»

цифровых технологий компаниями, получившими поддержку в рамках федерального проекта «Цифровые технологии», процент», «Методикой расчета показателя «Количество PCT-заявок по «сквозным» цифровым технологиям, поданных организациями, получившими поддержку в рамках национального проекта «Цифровая экономика», «процент») // СПС «КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&base=LAW&n=366350&demo=1 (дата обращения: 05.09.2022).

14. Об утверждении Плана противодействия коррупции ФАС России на 2021–2024 годы в нем Применение цифровых технологий в целях противодействия коррупции и разработка мер по противодействию новым формам проявления коррупции, связанным с использованием цифровых технологий»: Приказ ФАС от 30.09.2021 № 1054/21 // СПС «КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&base=LAW&n=414916&demo=1 (дата обращения: 04.09.2022).

15. Ожегов С. И. Толковый словарь русского языка. Москва, 1992.

16. Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2019 год и на плановый период 2020 и 2021 годов (утв. Минфином России) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=308390#0GS 2ZGT0K5lxrJ9q (дата обращения: 05.09.2022).

17. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н. А. Голованова, А. А. Гравина, О. А. Зайцев и др. Москва: ИЗиСП, КОНТРАКТ, 2019. 212 с.

18. Чермянинов Д. В. Информационные и цифровые технологии в таможенном регулировании: суть и соотношение понятий // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2018. Т. 4, № 4. С. 133–145.

Н. Ф. Гуломова,
доктор экономических наук, PhD,
директор Индийско-Узбекского центра информационных технологий,
Ташкентский университет информационных технологий
имени Мухаммада аль-Хорезми

ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ В ПРОЦЕССЕ ПЕРЕХОДА К ЦИФРОВОЙ ЭКОНОМИКЕ В УЗБЕКИСТАНЕ: РОСТ УГРОЗ КИБЕРБЕЗОПАСНОСТИ

Аннотация. Экспоненциальный рост взаимосвязей в Интернете привел к значительному росту угроз кибербезопасности. Совершенствование правового регулирования, а также разработка более инновационных и эффективных механизмов защиты от киберпреступлений считается необходимой потребностью в кибербезопасности. В данной статье рассмотрены проблемы кибератак, возникающие в процессе перехода к цифровой экономике, и меры по обеспечению кибербезопасности в Узбекистане.

Ключевые слова: киберпреступление, кибербезопасность, цифровая экономика, проблемы, кибератаки, правовые механизмы

PROBLEMS ARISING IN THE PROCESS OF TRANSITION TO THE DIGITAL ECONOMY IN UZBEKISTAN: THE RISE OF CYBERSECURITY THREATS

Abstract. The exponential growth of interconnections on the Internet has led to a significant increase in cybersecurity threats. Improving legal regulation, as well as developing more innovative and effective mechanisms for protecting against cybercrime, is considered a necessary need for cybersecurity. This article discusses the problems of cyber-attacks that arise in the process of transition to a digital economy and measures to ensure cyber security in Uzbekistan.

Keywords: Cybercrime, Cybersecurity, Digital economy, Problems, Cyberattacks, Legal mechanisms

Киберпреступность становится все более организованной, о чем свидетельствует рост числа инцидентов. В 2021 г. среднее количество кибератак и утечек данных увеличилось на 15,1 % по сравнению с предыдущим годом [1]. В эпоху глобализации безналичная оплата становится реальностью. Однако цифровая экономика, состоящая из взаимосвязанных электронных кошельков, социальных сетей и мобильного банкинга, создала условия для процветания киберпреступности в Узбекистане. Киберпреступления выступают как угроза развитию цифровой экономики. Для кражи денег с электронных кошельков людей появилась новая технология, в которой хакеры и мошенники используют фишинг. вымогательство (кибервымогательство) путем угрозы завладения и раскрытия личной информации; запугивание с применением насилия, оскорбления в социальных сетях (кибербуллинг) и т. п. Кроме того, все более серьезными становятся риски, связанные с повреждением и потерей информации из-за вирусных заражений каналов связи и баз данных. Банковский и финансовый секторы становятся все более привлекательными для злоумышленников. После недавних атак на финансовые учреждения и массового переноса услуг онлайн-банкинга в эпоху карантина все больше экспертов сходятся во мнении, что киберугрозы становятся ключом к финансовой стабильности банков и финансовых служб.

По мере развития информационных технологий возрастает и уязвимость киберпространства и его базовой инфраструктуры для широкого спектра рисков, связанных как с физическими, так и с киберугрозами и опасностями. Использование данных уязвимостей позволит злоумышленнику получить удаленный доступ к информационной системе или веб-сайту, а также к файлам и информации, что в свою очередь может привести к утечке персональных данных 2 026 824 граждан Республики Узбекистан. Так, согласно данным 2019 г., в информационных системах и на веб-сайтах национального сегмента сети Интернет выявлено 268 инцидентов, 816 уязвимостей и около 132 000 угроз кибербезопасности [2]. В Узбекистане за 2020 г. было выявлено более 27 000 000 событий вредоносной и подозрительной сетевой активности, исходящей из адресного пространства сегмента сети Интернет, которые в свою очередь представляют угрозу безопасному

и стабильному функционированию информационных систем и ресурсов. В стране только в 2020 г. было выявлено почти 8 млн инцидентов информационной безопасности, часть из которых имели критический уровень. Для минимизации рисков в ближайшие 3–5 лет цифровые технологии должны стать предметом национального и наднационального регулирования в Узбекистане; в то же время должны быть введены защитные меры для продвижения отечественных услуг на международный рынок.

Скорость интернет-соединения в Узбекистане остается относительно низкой, имеет плохое качество связи и происходят частые отключения [3]. Сбои в программном обеспечении, кибератаки, аварии, отключение электричества могут парализовать работу государственных органов, социальных бюджетных учреждений, отдельных предприятий, нанося им значительный экономический ущерб. Так, в качестве примера можно привести блэкаут, произошедший в январе 2022 г. в Узбекистане. Крупная авария, которая началась в энергосистеме Узбекистана, оставила жителей страны без света и охватила три страны Центральной Азии. По данным Минэнерго, возобновление подачи электричества по всему Узбекистану заняло около 53 часов [4].

Правовой основой, регулирующей сферу развития и цифровизации информационно-коммуникационных технологий, являются законы Республики Узбекистан «О связи», «О телекоммуникациях», «О государственных закупках», «Электронная коммерция», «Об электронных цифровых подписях» и «Об электронном документообороте» [5]. Большинство этих правовых документов приняты в период с 2000 по 2005 г., касающихся развития цифровой экономики, не учитывают тенденции развития в сфере ИКТ. Цифровая экономика изучается в областях гражданского права, интеллектуального права, налогового права, кибербезопасности.

На сегодняшний день в соответствии с современными тенденциями, вызовами и угрозами в области информационных технологий, популяризации киберпреступлений в связи с развитием глобальной сети Интернет законодательство Узбекистана вышло на новый уровень своего развития. В целях регулирования отношений в области персональных данных и их защиты 2 июля 2019 г. был принят Закон Республики Узбекистан «О персональных данных».

Кибербезопасность в Узбекистане регулируется Законом «О кибербезопасности», подписанным Президентом Республики Узбекистана от 15 апреля 2022 г. Закон состоит из 8 глав и 40 статей. На практике основная часть киберпреступлений, а именно 90 % экономических преступлений в киберпространстве связаны с электронной коммерцией. Именно на электронной торговой площадке могут возникнуть всевозможные кибератаки. Электронная коммерция регулируется Законом Республики Узбекистан «Об электронной коммерции». Использование в качестве пространства информационных систем с учетом особенностей заключения договора в электронной коммерции (путем осуществления акцепта в виде электронного документа или электронного сообщения) является предпосылкой возможной потенциальной угрозы киберпреступности в данной сфере. Уголовным кодексом Республики Узбекистан предусмотрены такие компьютерные преступления, как грабеж с использованием компьютер-

ной техники, растрата или взлом, кража путем несанкционированного доступа к компьютерной системе, незаконный сбор информации, ее разглашение или использование. В настоящее время в Узбекистане действует законодательство о преступлениях в области кибербезопасности, и государственные центры работают над регулированием этой сферы. UZ-CERT создана в целях обеспечения реализации постановления Президента Республики Узбекистан от 5 сентября 2005 г. № 167 «О дополнительных мерах по обеспечению компьютерной безопасности национальных информационно-коммуникационных систем» восстановление данных. Однако современная тенденция развития требует необходимости создания центров кибербезопасности на сетевой основе. Кроме того, необходимо дальнейшее изучение данной области с правовой точки зрения, разработка стандартов кибербезопасности для организаций, а также национальных программ кибербезопасности и стандартов показателей кибербезопасности. Благодаря последним реформам в области правового регулирования вопросов цифровизации Узбекистан улучшил свою позицию в Глобальном индексе кибербезопасности.

Индекс и рэнкинг кибербезопасности стран (Global Cybersecurity Index (GIC))

Страна	Индекс GIC	Рэнкинг на глобальном уровне	Рэнкинг среди стран СНГ	Правовые меры	Технические меры	Организационные меры	Развитие потенциала	Сотрудничество
Российская Федерация	98,06	5	1	20,00	19,08	8,98	20,00	20,00
Беларусь	50,57	89	5	10,36	9,50	8,31	7,88	14,51
Казахстан	93,15	31	2	20,00	19,54	18,46	15,15	20,00
Армения	50,47	90	6	12,87	13,86	4,87	7,85	11,02
Узбекистан	71,11	70	4	19,27	12,56	10,05	15,68	13,56
Киргизская Республика	49,64	92	7	13,43	7,85	14,37	1,87	12,11

Разработано автором на основе [6].

Узбекистан занял 70-е место, индекс Узбекистана составил 71,11 балла из максимальных 100. В частности, Узбекистан получил 19,27 балла в сегменте правовых мер, 10,05 балла – в сегменте организационных мер, 12,56 балла – в сегменте технических мер, 15,68 балла – в сегменте по развитию потенциала и 13,56 бал-

ла – в сегменте сотрудничества. За три года Узбекистан значительно улучшил свою позицию в рейтинге стран по уровню кибербезопасности, поднявшись с 92-го (2017 г.) на 70-е (2020 г.) место. Однако по показателям технических и организационных мер и партнерству в области кибербезопасности страна немного отстает, и необходимо улучшить данные показатели, направленные на обеспечение информационной безопасности.

В силу своей специфики лишь принятия и осуществления национальных законов недостаточно для решения современных проблем кибербезопасности. Транснациональный характер киберпреступлений требует эффективного решения проблемы кибербезопасности с налаживанием партнерских отношений между государственным и частным секторами, а также международного сотрудничества с созданием единой нормативной базы, которая должна выполнять роль ключевого компонента стратегий по обеспечению кибербезопасности.

Таким образом, в настоящее время в Узбекистане действуют законы о кибербезопасности, и государственные центры работают над регулированием этой сферы. Современная тенденция развития требует необходимости создания центров кибербезопасности на сетевой основе. Кроме того, необходимо дальнейшее изучение данной области с правовой точки зрения, разработка стандартов кибербезопасности для организаций, а также разработка национальных программ кибербезопасности и стандартов показателей кибербезопасности. По этой причине совершенствование норм Гражданского, Налогового кодексов и других нормативно-правовых документов Республики Узбекистан требует учета процессов цифровой экономики.

Список литературы

1. Chuck Brooks Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know. 2022. URL: https://www.forbes.com/

2. Гафуров К. Роль диджитализации в образовании при подготовке юристов и политика Узбекистана в борьбе с киберпреступлениями // Журнал правовых исследований. 2020. № 10. С. 39–46.

3. Ookla: Internet speed in Uzbekistan is getting even worse Интернет-издание kun.uz от 22.11.2018. URL: https://m.kun.uz/en/news/2018/11/22/

4. Блэкаут 25 января начался с Узбекистана – межгосударственная комиссия // Spot. 16.03.2022. URL: https://www.spot.uz/ru/2022/03/16/blackout-start/

5. Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/

6. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-c

И. И. Гусева,
кандидат юридических наук, доцент,
доцент кафедры уголовно-процессуального права и криминалистики,
Владимирский юридический институт
Федеральной службы исполнения наказаний России,
А. В. Ионова,
магистрант,
Владимирский юридический институт
Федеральной службы исполнения наказаний России

ЦИФРОВИЗАЦИЯ УГОЛОВНОГО ПРОЦЕССА В СОВРЕМЕННЫХ УСЛОВИЯХ

Аннотация. Рассматриваются вопросы, связанные с необходимостью расширения возможностей применения IT-технологий в уголовно-процессуальной деятельности. Анализируются отдельные аспекты цифровизации досудебных стадий уголовного дела. Обращается внимание на недостаточность программирования процедур на стадии возбуждения уголовного дела. Делается вывод о целесообразности скорейшего усовершенствования программных продуктов и законодательной базы для более широкого использования цифровых технологий в досудебном производстве по уголовному делу.

Ключевые слова: цифровые технологии, информационные технологии, программный продукт, цифровая трансформация, принятие сообщений о преступлении, оптимизация, стадия возбуждения уголовного дела

DIGITALIZATION OF THE CRIMINAL PROCESS IN MODERN CONDITIONS

Abstract. The issues related to the need to expand the possibilities of using IT technologies in criminal procedural activities are considered. Separate aspects of digitalization of pre-trial stages of a criminal case are analyzed. Attention is drawn to the insufficiency of programming procedures at the stage of initiation of a criminal case. Делается вывод о целесообразности скорейшего усовершенствования программных продуктов и законодательной базы для более широкого использования цифровых технологий в досудебном производстве по уголовному делу.

Keywords: Digital technologies, Information technology, Software product, Digital transformation, Accepting reports of a crime, Optimization, Stage of initiation of a criminal case

Современный этап развития общества стал немыслим без применения цифровых технологий в различных отраслях жизнедеятельности [4]. Такие явления затронули и уголовно-процессуальную сферу, в рамках которой используются отдельные возможности цифровизации. Однако в основном применение технических и информационных технологий затронуло судебные стадии.

Не вызывает сомнений, что применение информационных технологий в уголовно-процессуальной деятельности предоставляет возможность стабильного обе-

спечения различного рода процессуальных правил и требований, сокращает сроки производства, а, в отдельных случаях, позволяет повысить уровень объективности и безопасности такой деятельности.

В научной литературе поддерживается справедливое мнение, высказанное в рамках проведенного в 2017 г. Байкальского юридического форума, что последующее совершенствование уголовно-процессуальной деятельности, в том числе на стадии возбуждения уголовного дела, представляется возможным, лишь ориентируясь на уровень технического развития современного общества [3]. Направления использования таких средств в рамках уголовно-процессуальной деятельности являются различными. Рассматривая досудебное производство, О. В. Химичева, А. В. Андреев представляют возможным говорить об их применении в криминалистических целях – поиск доказательств, их исследование, изъятие и т. д., в большей части, по преступлениям, совершенным с использованием IT-технологий. Ими обращается внимание на ряд неразрешенных на законодательном уровне вопросах, затрудняющих процедуру изъятия и приобщения к уголовному делу криптовалют, документов, исполненных только в электронном виде и подписанных электронной подписью, информации, содержащейся в «облачных» хранилищах [6. С. 22–23].

В научной литературе обоснованно фиксируется необходимость использования электронных технологий для урегулирования вопросов процедурного характера, например, для фиксации поступившей информации, возможности организации осуществления процессуальных действий и т. п. Наращивание способов применения цифровых технологий предоставляют возможность оптимизировать уголовно-процессуальную деятельность, в том числе и на стадии возбуждения уголовного дела, без изменения его предназначения и основной сущности.

Учитывая увеличение уровня воздействий на уголовный процесс информационных технологий, в научных кругах на протяжении около десяти лет нарастает внимание к этим вопросам. Аналогичные дискуссии ведутся и в других странах, где пристальное внимание уделяется важности переосмысления уголовно-процессуальных теорий. Особый интерес вызывают не только сложности технических разработок отдельных процессов, но и вопросы законодательной фиксации в уголовно-процессуальной деятельности средств цифровизации и создания уголовного процесса, перешедшего на совершенно иной, новый уровень.

Критикуя высказывания о создании нового уголовного процесса в связи с внедрением цифровых технологий, Л. В. Головко констатирует отсутствие необходимости в замене существующего классического уголовного процесса на процесс, подверженный воздействию цифровых технологий. Следует согласиться с его видением цифровизации в уголовном процессе на современном этапе как довольно рутинной и локальной оптимизации отдельных процессуальных институтов и форм [1. С. 24–25].

В настоящее время целесообразно говорить исключительно о некоторых направлениях цифровизации на досудебных стадиях уголовного процесса. Прежде всего, положительную роль в совершенствовании уголовного процесса может сыграть его ведение в электронном формате при помощи применения специальной программной оболочки. Кроме этого, представляется возможным и необходимым проведение мо-

дернизации системы автоматизированных рабочих мест. Положительных результатов можно добиться при рационализации процедуры осуществления процессуальных действий в стадиях возбуждения уголовного дела и предварительного расследования посредством более интенсивного использования информационных технологий. Ряд авторов указывают, что цифровизация является предпосылкой для повышения уровня доступности, открытости и оперативности российского правосудия за счет уменьшения уровня его избыточного формализма [5. С. 137–138].

В первую очередь, на наш взгляд, следует усовершенствовать программное обеспечение для подачи заявления (сообщения) о преступлении. В настоящее время имеется возможность подачи заявлений в электронной форме, но они рассматриваются как жалоба, а не в рамках уголовно-процессуального кодекса как повод к возбуждению уголовного дела [2. С. 98–99]. Соответственно для этого требуется и внесение дополнений, как минимум, в ст. 141, 142, 144, 474.1 УПК РФ. Полагаем целесообразным допустить в отдельных случаях производство следственных и процессуальных действий в электронном формате. Заслуживает внимания применение специальной программной оболочки, за счет которой появится возможность размещения материалов соответствующего уголовного дела с возможностью дополнения в него информации при осуществлении действий процессуального характера в онлайн-режиме. Для обеспечения безопасности такая система должна содержать уровни доступа: для лиц, желающих ознакомиться с материалами уголовного дела; для органов и должностных лиц, осуществляющих надзорные и контрольные функции; для обеспечения взаимодействия между правоохранительными органами и структурами.

Такая организация позволит сократить время, необходимое для совершения различных процессуальных действий и осуществления согласования принимаемых решений. Кроме того, программная оболочка такого формата предоставит возможность более быстрой подготовки документов процессуального характера посредством применения ранее сохраненных в системе форм, вносить корректировки в случае совершения технических ошибок, а также выдавать копии [7. С. 214–216].

Формулируя итоги, отметим, что осуществление уголовно-процессуальной деятельности в цифровом формате предоставит возможность оптимизировать работу сотрудников правоохранительных органов: следователя, дознавателя, повысить уровень функционирования системы гарантий правового статуса личности, сделать более удобным использование результатов такой деятельности, а также осуществлять взаимодействие между различными структурами и органами на удаленной основе. В конечном счете, все это поможет укрепить законность такой деятельности в силу повышения эффективности ведомственного контроля и прокурорского надзора. Внедрение современных технологий должно идти в ногу с соблюдением принципа законности, а не стать бездумной гонкой за научно-техническим процессом.

Список литературы

1. Головко Л. В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15–25.

2. Гусева И. И., Зубков В. Н. Поводы к возбуждению уголовного дела: перспективы расширения и цифровизации // Modern Science. 2022. № 4–1. С. 96–99.

3. Итоги. Байкальский юридический форум. 21–22 сентября 2017. URL: http://blf.bgu.ru/rezults.aspx (дата обращения: 10.09.2022).

4. О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203. URL: http://publication.pravo.gov.ru/Document/View/0001201705100002 (дата обращения: 10.09.2022).

5. Пшава В. В., Соколов А. Б., Галдина Э. О. К вопросу о цифровизации уголовного процесса // Право и практика. 2022. № 2. С. 135–138.

6. Химичева О. В., Андреев А. В. Цифровизация как тренд развития современного уголовного процесса // Вестник Московского университета МВД России. 2020. № 3. С. 21–23.

7. Чурикова А. Ю. Проблемы цифровизации российского уголовного процесса // Вестник Саратовской государственной юридической академии. 2021. № 6 (143). С. 209–216.

Г. С. Девяткин,
кандидат юридических наук, доцент,
Московский институт электронной техники

НЕКОТОРЫЕ ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ПРОБЛЕМЫ ВОЗБУЖДЕНИЯ И РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ, СВЯЗАННЫХ С ХИЩЕНИЕМ КРИПТОВАЛЮТ

Аннотация. За последние три года рост киберпреступлений в России составил почти 400 %, и в 2021 г. уже каждое четвертое преступление включало приставку «кибер». Одновременно с этим общество активно интересуется цифровыми активами, почти у 15 млн граждан в том или ином объеме есть доступ к криптовалютам. Несмотря на определенные правовые пробелы, связанные с регулированием криптовалют и постоянным обсуждением предстоящих изменений в их правовом статусе, преступления, связанные с хищением криптовалют, демонстрируют устойчивый рост. В настоящей статье рассмотрены правовые и организационные проблемы, связанные со стадиями возбуждения и предварительного расследования уголовных дел, связанных с хищением криптовалют.

Ключевые слова: высокотехнологичное право, цифровые технологии, криптовалюта, возбуждение уголовного дела, предварительное расследование, цифровые активы

SOME LEGAL AND ORGANIZATIONAL PROBLEMS OF INITIATION AND INVESTIGATION OF CRIMINAL CASES RELATED TO THE THEFT OF CRYPTOCURRENCIES

Abstract. Over the past three years, the growth of cybercrimes in Russia has amounted to almost 400 %, and in 2021 already every fourth crime included a «prefix» cyber. At the same time, the society is actively interested in digital assets, almost 15 million citizens have access to cryptocurrencies in one volume or another. Despite certain legal gaps related to the regulation of cryptocurrencies and the constant discussion of upcoming

changes in their legal status, crimes related to the theft of cryptocurrencies are showing steady growth. This article discusses the legal and organizational problems associated with the stages of initiation and preliminary investigation of criminal cases related to the theft of cryptocurrencies.

Keywords: High-tech law, Digital technologies, Cryptocurrency, Initiation of criminal proceedings, Preliminary investigation, Digital assets

Различные виды хищений традиционно являются одним из самых распространенных преступлений в России. Существующие методики расследования, выработанные десятилетиями практики в совокупности с серьезными научными исследованиями и полученным образованием, позволяют органам следствия достаточно эффективно раскрывать преступления, предусмотренные ст. 158, 159 Уголовного кодекса РФ.

Однако за последние несколько лет все чаще предметом хищений являются криптовалюты. Государство, принимая на себя обязательства, связанные с уголовно-правовой защитой граждан, общества, достаточно избирательно подходит к вопросам возбуждения и расследования уголовных дел, в которых у потерпевших была похищена криптовалюта.

Понятия и нормативно-правовое регулирование. В законодательстве отсутствует термин «криптовалюта». Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [7] не закрепил легальное определение криптовалютам, ограничившись понятием «цифровая валюта», что с технической точки зрения не является тождественным понятию «криптовалюты». При этом анализ статей данного Федерального закона позволяет указать на достаточно подробное объяснение законодателем процессов, связанных с оборотом цифровой валюты (ст. 14): организация выпуска, выпуск, организация обращения. Однако определение «цифровой валюты», которое закреплено в ст. 3, с технической точкой зрения не коррелирует с процессами оборота цифровой валюты, которые мы находим в ст. 14.

Если речь в рассматриваемом федеральном законе идет именно о цифровой валюте, то что следует включать в ее трактовку не на нормативном уровне, а на понятийном? Каким образом объяснить сотруднику органов следствия, что у потерпевшего была похищена цифровая валюта и необходимо возбуждать уголовное дело со всеми соответствующими последствиями? Игра терминами, когда государство не включает в законодательство отдельное определение «криптовалюта», а вводит понятие «цифровая валюта», позволяет не реагировать правоохранительным органам на сообщения о хищении криптовалют. Здесь важно отметить технические особенности природы рассматриваемых определений: цифровая валюта централизована, существует строго определенная группа людей и сеть технических устройств, которые контролируют сетевые транзакции. Для криптовалют отсутствует так называемый центральный сервер, децентрализация является ключевым фактором отличия с цифровой валютой. Криптовалюта не принадлежит отдельному государству, цифровая валюта может быть выпущена центральным банком или иным уполномоченным органом. Возможно, по этой причине законодатель избегает использования термина «криптовалюта», а вводит определение «цифровая валюта».

Однако отсутствие нормативного закрепления криптовалюты не ограничивает правоприменителя на практике. Так, еще в мае 2018 г. Девятый арбитражный апелляционный суд впервые обязал должника предоставить конкурсному управляющему доступ к содержимому криптокошелька для включения его в конкурсную массу [3]. В указанном судебном акте фактически суд указал на право лица «по своему усмотрению владеть, пользоваться, распоряжаться содержимым криптокошелька как своим собственным имуществом, совершать в отношении него любые действия, не противоречащие закону и иным правовым актам и не нарушающие права и охраняемые законом интересы других лиц».

Одновременно с примерами из судебной практики действует правило, согласно которому финансовая система страны является объектом правовой охраны публичного права, и неурегулированное правовое положение криптовалюты позволяет следственным органам квалифицировать ее как «денежный суррогат». Подтверждением избирательного подхода правоприменителя при рассмотрении вопросов об уголовном преследовании лиц по уголовным делам, связанных с криптовалютой, является решение Петроградского районного суда г. Санкт-Петербурга, который признал именно криптовалюту (не цифровую валюту и не цифровые финансовые активы) имуществом по уголовному делу.

Фабула состояла в следующем. В 2017 г. потерпевший приобрел 7000 монет криптовалюты эфириум (ETH). Обвиняемый В. незаконным путем получил доступ к данному кошельку с криптовалютой и заблокировал доступ к нему потерпевшему. После этого обвиняемый перевел монеты на свои кошельки. При рассмотрении уголовного дела суд указал, что криптовалюта имеет ценность, она может быть предметом преступления. [5]

Отдельно следует отметить, что в Постановлении Пленума Верховного суда РФ от 7 июля 2015 г. № 32 предусмотрена формулировка: «предметом преступлений, предусмотренных ст. 174 и 174.1 Уголовного кодекса РФ, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления» [6].

Кроме того, государство обязало некоторых государственных служащих подавать сведения о цифровой валюте начиная с 2021 г. На практике наличие криптовалюты попадает под это требование. Также некоторым государственным служащим и лицам, которым не разрешается иметь зарубежные счета, запрещено владеть цифровой валютой, которая выпущена в иностранных информационных системах.

Сложилась ситуация, при которой цифровая валюта обладает нормативным закреплением, однако на практике субъекты правоприменения подменяют ее криптовалютой, которая по своей природе отлична от цифровой.

Необходимо безусловное признание криптовалют на законодательном уровне с внесением соответствующих поправок в Уголовный кодекс, Уголовно-процессуальный кодекс и иные нормативно-правовые акты. Существующие правовые неопределенности не обеспечивают гарантии защиты лиц, потерпевших от преступлений.

Возбуждение и расследование уголовных дел, связанных с хищением криптовалют. Работники органов следствия указывают на особую сложность при выявлении преступлений, совершаемых с использованием криптовалюты [1. С. 16].

В эпоху высокотехнологичного права необходимы соответствующие знания у органов следствия [2]. На практике встречаются ситуации, когда должностное лицо, принимающее заявление о преступлении не имеет представления о том, что такое криптовалюта, как устроена технология «блокчейн» и система децентрализации.

Одна из главных проблем на первоначальном этапе проверки заявления о преступлении и решении вопроса о возбуждении уголовного дела заключается в установлении размера похищенной криптовалюты, а также принадлежности ее заявителю.

Механизм транзакций с использованием криптовалюты устроен так, что он делает крайне сложным контроль со стороны банков или государственных органов. Не во всех случаях потерпевший в действительности готов подтвердить факт наличия у него похищенной криптовалюты. Цифровые следы не удается установить и непросто добиться возбуждения уголовного дела. Вано понять, где хранилась криптовалюта.

В зависимости от выбранного типа, могут использоваться криптобиржи и криптокошельки кастодиального типа. В этом случае криптовалюта и транзакции по ней контролируются операторами. С позиции безопасного хранения криптовалюты наличие третьих лиц, имеющих доступ к транзакциям, не самое лучшее решение. Однако в случае кражи биржа предоставит правоохранительным органам цифровые следы по транзакциям с похищенной криптовалютой. Некастодиальные криптокошельки и ключи к ним хранятся вне бирж, нередко это флеш-накопители, без которых доступ к криптовалюте невозможен. Однако при хищении такой флешки потерпевший фактически теряет шансы на установление принадлежности похищенной криптовалюты. Разновидность некастодиальных криптокошельков: «горячие» (с доступом через мобильное приложение) и «холодные» (аппаратные, доступ через флеш-накопитель).

Возврат похищенной криптовалюты. Одна из распространенных проблемных ситуаций при расследовании преступлений, связанных с хищением криптовалюты, связана с возвратом потерпевшему похищенной суммы. В некоторых случаях обвиняемый соглашается добровольно осуществить транзакцию с криптокошелька. Но это исключение из правила, такая ситуация произошла в Беларуси [4]. Проведение обысков, направленных на поиск похищенного, не дает результатов. В том случае, если был похищен флеш-накопитель с доступом к «холодному» криптокошельку, у органов следствия повышаются шансы на успех при проведении следственных действий.

Распространены ситуации установления органами следствия цифровых следов транзакций на криптобиржах. Возврат похищенных средств происходит за счет заморозки счета путем направления соответствующего процессуального документа руководству криптобиржи. Однако криптобиржа может отказать в запросе. Особенно это актуально в странах Восточной Европы, куда обращаются российские правоохранительные органы. В этих государствах криптобирржи нередко находятся в «серой» зоне и не регулируются национальным законодательством.

При выводе обвиняемым похищенной криптовалюты через обменники (в большинстве своем их деятельность незаконна) и конвертации в обычную валюту, возврат похищенной суммы может производиться уже в итоговой конвертируемой денежной массе. Основная сложность при этом заключается в установлении происхождения наличных, изъятых у обвиняемого. Нередко правоохранительные

органы привлекают для возврата похищенной криптовалюты частные организации, специализирующиеся на информационной безопасности и расследовании киберпреступлений и инцидентов.

Еще одной сложностью при возврате похищенной криптовалюты является использование обвиняемым специальных технических средств «миксеров», с помощью которых искомые транзакции по выводу средств «разбавляются» иными операциями, что приводит к значительному усложнению цепочки преступления.

Помимо криптовалют предметом хищения могут выступать стейблкоины: разновидность криптоактивов с привязкой стоимости к обычной валюте. Сложилась ситуация, при которой законодатель поставил судебную защиту цифровых валют (не криптовалют, о которых ничего нет) в зависимость от того, была ли она ранее задекларирована. Согласно содержанию ст. 1, 14 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», из-под понятия цифровые валюты выпадают такие распространенные криптоактивы как стейблкоины USDT, BUSD, криптовалюта Ripple (XRP) и целый ряд других криптоактивов, которые были эмитированы централизованно, но не на объектах российской информационной инфраструктуры. К цифровым финансовым активам указанные криптоактивы также не могут быть отнесены ввиду несоответствия и их критериям тоже.

Подводя итог, следует отдельно отметить проблему переподготовки следователей для расследования преступлений, связанных с хищением криптовалют. Методические рекомендации не заменяют полноценного обучения с моделированием киберпреступлений на специальных стендах.

Несмотря на создание отделов внутри структуры Следственного комитета РФ, ориентированных на расследование киберпреступлений, требуется масштабное переподготовка во всех органах следствия и дознания, а также среди государственных обвинителей, судей, адвокатов. Принятие изменений в нормативно-правовую базу вопрос ближайших двух-трех лет, но к этому моменту уже необходимо наличие новых кадров.

Список литературы

1. Багмет А. М. К вопросу выявления и расследования преступлений, совершаемых с использованием криптовалюты // Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола» (Москва, 25 апреля 2019 г.) / под общ. ред. А. М. Багмета. Москва: Московская академия Следственного комитета Российской Федерации, 2019. С. 13–17.

2. Бертовский Л. В. Понятие высокотехнологичного права // Высокотехнологичное право: генезис и перспективы: материалы II Международной межвузовской научно-практической конференции (Москва – Красноярск, 26 февраля 2021 г.). Красноярск: Красноярский государственный аграрный университет, 2021. С. 43–47.

3. Дело № А40–124668/2017. Девятый арбитражный апелляционный суд. URL: https://ras.arbitr.ru/

4. Новикова И. В. Государственное регулирование криптовалют: теоретические подходы и опыт Республики Беларусь // Технология блокчейн и криптовалютный

рынок: глобальные риски, тенденции и перспективы развития: сборник научных трудов. Москва: Институт научной информации по общественным наукам РАН, 2022. С. 153–175.

5. Новости Генеральной прокуратуры РФ. URL: https://epp.genproc.gov.ru/web/proc_78/mass-media/news?item=73895418

6. Постановление Пленума Верховного Суда РФ «О внесении изменений в Постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» от 26.02.2019 № 1.

7. Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ.

Е. В. Демидова-Петрова,
доктор юридических наук, доцент, заслуженный юрист, начальник кафедры уголовного процесса,
Казанский юридический институт Министерства внутренних дел Российской Федерации

КРИМИНОЛОГИЧЕСКИЙ ПОРТРЕТ НЕСОВЕРШЕННОЛЕТНЕГО ПРЕСТУПНИКА В СОВРЕМЕННОЙ РОССИИ (ПОД ВОЗДЕЙСТВИЕМ ИНТЕРНЕТ-ПРОСТРАНСТВА)

Аннотация. Настоящая статья посвящена особенностям криминологического портрета несовершеннолетнего преступника. Целью работы явилось получение новых знаний о влиянии интернет-пространства, онлайн социальной среды на формирование личности современного преступника, не достигшего совершеннолетия. Приведены полученные автором результаты исследования особенностей лиц несовершеннолетнего возраста, совершивших преступные деяния. Отдельное внимание уделено оказываемому влиянию интернет-пространства, онлайн социальной среды на формирование, развитие личности несовершеннолетнего преступника.

Ключевые слова: несовершеннолетний, преступность несовершеннолетних, социальная среда, интернет-пространство, личность преступника, цифровизация, глобализация

CRIMINOLOGICAL PORTRAIT OF A MINOR CRIMINAL IN MODERN RUSSIA (UNDER THE INFLUENCE OF THE INTERNET SPACE)

Abstract. This article is devoted to the peculiarities of the criminological portrait of a juvenile criminal. The purpose of this work was to gain new knowledge about the influence of the Internet space, the online social environment on the formation of the personality of a modern criminal who has not reached adulthood. The results obtained by the author of the study of the characteristics of persons of juvenile age who have

committed criminal acts are presented. Special attention is paid to the influence of the Internet space, the online social environment on the formation and development of the personality of a juvenile offender.

Keywords: Juvenile, Juvenile delinquency, Social environment, Internet space, criminal identity, Digitalization, Globalization

Преступность лиц несовершеннолетнего возраста всегда вызывала и продолжает вызывать особый интерес ученых и практиков. Еще в более ранних работах автора было отмечено: «Именно лица несовершеннолетнего и молодого возраста являются самыми динамично развивающимися и трансформирующимися категориями населения. Именно на несовершеннолетний и молодежный возраст приходится несколько смен социальных ролей (ученик начальной, средней школы, учащийся высшего учебного заведения, колледжа, техникума, молодой специалист, создание собственной семьи, рождение детей и их воспитание)» [1]. Такие трансформации сопряжены с различными кризисными становлениями личности.

В молодежной стратегии ООН «Молодежь-2030» приводятся данные, указывающие что на сегодняшний день в мире проживает 1,8 млрд лиц молодого возраста. Данные показатели являются одними из наиболее высоких за всю историю развития человечества. Также в данной стратегии [2] отмечен перечень основных направлений, связанных с повышением качества уровня жизни лиц молодого возраста. Среди которых важно отметить следующие:

– привлечение лиц молодого возраста к решению важных современных проблем (достижение мира, справедливости, безопасности);

– доступность здравоохранения, образования;

– улучшение экономического (материального) положения лиц молодого возраста;

– обеспечение достойных условий реализации политических, и гражданских прав лицами молодого возраста;

– обеспечение поддержки лиц несовершеннолетнего и молодого возраста в различных ситуациях конфликтов и кризисов.

Необходимо выделить и тот факт, что за последние годы достаточно ярко выделился, затронув практически все сферы жизни современного человека и общества в целом, процесс цифровизации.

Сегодня цифровизация также в значительной степени влияет и на все категории населения. Данный процесс оказывает особое, значительное влияние именно на лиц несовершеннолетнего и молодого возраста.

Становится очевидным, что исследуемой нами сегодня категорией граждан становятся те лица несовершеннолетнего возраста, которые родились в мире, в котором существует интернет-пространство, онлайн социальная среда, которые уже не представляют возможным отсутствие онлайн социальных сетей, общения в онлайн-пространстве. При этом важно сказать, что, к сожалению, с процессом развития цифровизации начинает прослеживаться и возникновение влияния, носящего негативный характер на лиц несовершеннолетнего и молодого возраста.

Профессор Б. Я. Гаврилов в своих научных трудах справедливо указывает, на то, что некоторые отдельные процессы, носящие негативный характер, существующие

в современной жизни нашего общества, легли в основу и сделали жизнеспособным новый вид преступных деяний среди лиц несовершеннолетнего возраста – суицид [3].

В целях изучения криминологических особенностей личности несовершеннолетнего преступника автором настоящей статьи были разработаны анкеты, по которым были опрошены осужденные лица несовершеннолетнего возраста, которые состояли на учете в уголовно-исполнительных инспекциях УФСИН Российской Федерации в 72 субъектах России. В процессе проведения настоящего исследования особое внимание автора было обращено в сторону времяпровождения несовершеннолетних до момента совершения ими преступных деяний, за которые они были осуждены.

Ряд полученных данных о досуге лиц несовершеннолетнего возраста показал, что основное свободное время исследуемая категория граждан проводит в интернет-пространстве, онлайн социальной среде. То есть особой популярностью пользуются социальные сети, чаты, различные форумы, а также компьютерные игры.

Привлекла интерес и структура источников получения правовых знаний: более 50 % опрошенных получают их из средств массовой информации, а также из интернет-пространства, онлайн-пространства. 18 % осужденных несовершеннолетних указали такой вариант ответа: «как правило, ничего не делал». 72 % лиц несовершеннолетнего возраста указали досуг: «с друзьями на улице». Более 60 % опрошенных продемонстрировали компьютерную зависимость.

Нельзя не отметить и тот факт, что количество несовершеннолетних пользователей онлайн-пространства, социальных сетей стремительно увеличивается. Так, еще в 2010 г. 78 % российских школьников пользовались интернет-пространством, демонстрировали высокую коммуникативную активность в различных социальных сетях [4].

В 2013 г. количество лиц несовершеннолетнего возраста – пользователей социальных сетей возросло еще на 14 %. [5] Ранее Google и Ipsos было проведено совместное исследование, результаты которого показали, что 65 % россиян пользуются Интернетом ежедневно. При этом надо отметить, что лица несовершеннолетнего и молодого возраста «живут» в интернет-пространстве, пользуются Интернетом значительно больше [6].

Полученные результаты авторского исследования указывают на то, что современные лица несовершеннолетнего возраста проводят значительное количество своего свободного времени именно в интернет-пространстве, в онлайн социальных сетях. Естественно, подобное обстоятельство оказывает значительное влияние на формирование и развитие личности несовершеннолетнего. На сегодняшний день справедливо говорить о том, что информационному фактору, или онлайн-фактору, следует уделять отдельное внимание при рассмотрении комплекса причин, влияющих на личность несовершеннолетнего преступника. Так, говоря об особенностях криминологического портрета несовершеннолетнего преступника, важно подчеркнуть слабую защищенность указанной категории граждан от «опасностей», рисков, носящих различный характер, встречающихся в легкодоступном, зачастую анонимном мире онлайн. Именно в онлайн социальной среде лицо несовершеннолетнего возраста, и без того обладающее значительной виктимностью, становится еще более уязвимым, исходя из чего является жертвой преступных посягательств, что в перспективе ложится в основу совершения им преступных деяний.

Список литературы

1. Демидова-Петрова Е. В. Современные молодежные субкультуры криминальной и экстремистской направленности: особенности, виды // Мониторинг правоприменения. 2022. № 2 (43). С. 62–69.

2. Молодежь 2030. URL: https://www.un.org/youthenvoy/wp-content/uploads/2014/09/WEBR-UN-Youth-Strategy_Booklet_-Russian-for-WEB.pdf (дата обращения: 21.06.2022).

3. Гаврилов Б. Я. Суицид несовершеннолетних как форма отклоняющегося поведения в условиях современного общества: меры уголовно-правовой ответственности // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 4 (46). С. 463–471.

4. Солдатова Г. В., Зотова Е. Ю. Зона риска. Российские и европейские школьники: проблема онлайн-социализации // Дети в информационном обществе. 2011. № 7. С. 46–55.

5. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г. У. Солдатова, Т. А. Нестик, Е. И. Рассказова, Е. Ю. Зотова. Москва: Фонд Развития Интернет, 2013. 144 с.

6. Новое поколение интернет-пользователей: исследование привычек и поведения российской молодежи онлайн. URL: https://www.thinkwithgoogle.com/intl/ru-ru/insights-trends/user-insights/novoe-pokolenie-internet-polzovatelei-issledovanie-privychek-i-povedeniia-rossiiskoi-molodezhi-onlain/ (дата обращения: 01.06.2022).

Д. Е. Дроздов,
кандидат юридических наук,
Калужский государственный
университет имени К. Э. Циолковского

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРЕДУПРЕЖДЕНИЯ ЦИФРОВОЙ ПРЕСТУПНОСТИ

Аннотация. Исследована специфика современной преступности в цифровой среде и ее качества анонимности и латентности. Определены основные угрозы связанные с распространением идеологии экстремизма и терроризма, незаконным оборотом запрещенных предметов и веществ, легализацией доходов, полученных преступным путем. Предложены и обоснованы механизмы международного сотрудничества, связанные с обменом актуальной информацией и передовыми формами противодействия преступности.

Ключевые слова: цифровая преступность, цифровая среда, предупреждение преступности; профилактическая программа; терроризм, экстремизм, международное сотрудничество

THE MAIN DIRECTIONS OF DIGITAL CRIME PREVENTION

Abstract. The specifics of modern crime in the digital environment and its qualities of anonymity and latency are investigated. The main threats associated with the spread

of the ideology of extremism and terrorism, illegal trafficking of prohibited items and substances, legalization of proceeds from crime have been identified. Mechanisms of international cooperation related to the exchange of up-to-date information and advanced forms of crime prevention are proposed and substantiated.

Keywords: Digital crime, Digital environment, Crime prevention; Prevention program; Terrorism, extremism, International cooperation

Развитие наук уголовно-правового цикла обусловлено потребностями общества. Современная криминология находится в процессе накопления и систематизации знаний, что подразумевает не только уточнение предмета исследования и составных элементов, но и появление новых частных криминологических теорий. Подавляющее большинство сфер общественной полезной деятельности переходят в цифровую среду, что повышает вероятность возникновения угроз безопасности. В частности, вслед за ней, а зачастую опережая в цифровую среду проникает преступность, приобретая характер организованности, транснациональности и профессиональности, что значительно повышает ее опасность и увеличивает негативные последствия. Приобретая анонимность, обезличенность за счет специфики функционирования среды облегчается процесс совершения конкретного преступления и минимизируются издержки, в частности расширяются возможности и объемы распространения наркотических средств и психотропных веществ, финансирования террористический и экстремистской деятельности, легализации доходов полученных в результате совершения преступлений и т. д. Анонимность, отсутствие материальных следов преступной деятельности, трудности выявления и документирования особенно в случаях придания ей внешних признаков легальной деятельности стали причинами высокого уровня латентности.

Под преступностью традиционно понимается исторически изменчивое, неизбежное социально-правовое, относительно массовое явление, включающее совокупность запрещенных уголовным законом общественно опасных деяний, совершаемых в течение определенного периода времени на определенной территории [4. С. 57]. Качество исторической изменчивости наряду с научно-техническим прогрессом предопределили появление преступности в цифровой сфере, которая продолжает трансформироваться параллельно с совершенствованием информационных технологий.

Угрозы в цифровой сфере многообразны. Среди основных выделяются:

– Распространение идеологии терроризма и экстремизма, включая многообразие форм пропаганды не только с использованием социальных сетей и мессенджеров, но и онлайн-игр, позволяющих общаться в режиме реального времени.

– Незаконный оборот наркотических средств, психотропных веществ.

– Незаконный оборот оружия.

– Незаконный оборот материалов порнографического характера.

– Незаконный оборот криптовалют.

– Совершение преступлений, связанных с правом интеллектуальной собственности.

– Хакерские атаки на объекты инфраструктуры.

– Незаконный оборот конфиденциальной информации, включая получение прибыли.

– Преступления экономического характера, совершенные с использованием цифровых технологий.

– Общеуголовные преступления, совершенные с использованием цифровых технологий.

Действующее законодательство и правоприменительная практика динамично изменяются для обеспечения устойчивости системы противодействия распространению преступности в цифровой среде. Неслучайно целый раздел Стратегии национальной безопасности РФ посвящен информационной безопасности, где современные цифровые технологии рассматриваются как инструмент для вмешательства во внутренние дела государства. Отдельное внимание уделено распространению недостоверной, ложной информации, о заведомо ложных сообщениях об угрозе совершения террористических актов, призывах к участию в массовых беспорядка [1]. С учетом складывающихся условий, уголовной и административной ответственности, к примеру за распространение недостоверной информации явно недостаточно. Требуется нормативное закрепление механизма, определяющего привлечение к гражданско-правовой ответственности собственников цифровых СМИ, с законодательным определением размера компенсации вреда, причиняемого не только конкретному лицу, но и государственным интересам в целом.

Актуальной проблемой не только научного, но и практического характера выступает определение криминологических аспектов противодействия преступности в цифровом мире, направленном на создание условий для эффективного предупреждения преступлений, совершенных с использованием информационно-коммуникационных технологий. Работа правоохранительных органов требует оптимизации и трансформации в соответствии с новыми условиями. Усложнение правоохранительной деятельности определяется структурными изменениями, связанными с созданием новых, способных противодействовать высокотехнологичной преступности подразделений. Криминологическая реальность уже сейчас требует реформы уголовного права в части трансформации базовых уголовно-правовых институтов, криминализации новых общественно опасных деяний и уточнения признаков уголовно правовых запретов [3].

Традиционные формы и методы противодействия преступности в цифровой среде не обладают необходимым потенциалом и могут лишь использоваться как второстепенные инструменты. Совокупность передовых технологических методов, основанных на математическом моделировании с использованием ресурсов ЭВМ, направленных на масштабное изучение количественных и качественных изменений преступности и целью выявления существующих и только появившихся закономерностей преступности, составляют основу системы предупреждения преступности в цифровом мире. Обработка огромного массива информации открывает новые возможности прогнозирования преступности в краткосрочной, среднесрочной и долгосрочной перспективах. Следовательно, одной из приоритетных задач выступает достижение концептуального единства и преемственности с неоклассической криминологической теорией, продуцирования и применения новых цифровых методов и инструментов, основанных на совершенно новой теоретической базе [5. С. 423–430].

По данным Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, технологиями завтрашнего дня являются использование искусственного интеллекта в выявлении взаимосвязей злоумышленников. Как утверждают специалисты министерства, некоторые системы уже сейчас проводят биометрический анализ клавиатурного почерка пользователя или почерка движения мыши и т. д. Системы выявляют вредоносные веб-инъекции, социальную инженерию, фишинг, бот-сети, захват учетной записи, сети нелегального обналичивания денег и другие виды банковского мошенничества. В КНР разрабатывается система интеллектуального распознавания лиц, которая будет идентифицировать любого из 1,3 млрд жителей страны за 3 секунды даже при массовом скоплении населения. Компания «Лаборатория Касперского» встраивает модели машинного обучения в свои антивирусные продукты [2].

Международное сотрудничество в рамках государственной, правоохранительной, образовательной деятельности, своевременный обмен информацией о передовых формах противодействия преступности, научных достижениях, создающих основу для построения международной системы противодействия преступности. Координация совместной деятельности субъектов противодействия преступности на национальном уровне с определением прав, обязанностей, ответственности каждого и создание специализированного правоохранительного органа повысят эффективность противодействия преступности в цифровой сфере. Реалии современности определяют будущее за использованием программно-целевых методов воздействия на преступность. Программы профилактического воздействия на отдельные виды преступности реализуются на территории многих субъектов РФ и могут содержать профилактические мероприятия, предметом которых выступает цифровая преступность.

Список литературы

1. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 14.09.2022).

2. Справка по вопросу определения перечня перспективных информационных технологий для их инвестиционной поддержки и оценки информационной безопасности (федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» // Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru/uploaded/files/spravka-dlya-publikatsii-na-sajte.pdf (дата обращения: 19.09.2022).

3. Капинус О. С. Цифровизация преступности и уголовное право // Baikal Research Journal. 2022. Т. 13, № 1. DOI: 10.17150/2411–6262.2022.13(1).22. EDN: NZNOMN

4. Прозументов Л. М., Шеслер А. В. Криминология. Общая часть: учебник. Томск: ООО «ДиВо», 2007. С. 57.

5. Серебренникова А. В. Криминологические проблемы цифрового мира (цифровая криминология) // Всероссийский криминологический журнал. 2020. Т. 14, № 3. С. 423–430. DOI: 10.17150/2500–4255.2020.14(3).423–430.

А. С. Каменев,
адвокат,
Адвокатская палата Челябинской области

РЕФОРМИРОВАНИЕ ФУНКЦИИ ЗАЩИТЫ ПРИ ПЕРЕХОДЕ НА ЭЛЕКТРОННЫЙ ФОРМАТ ПРОИЗВОДСТВА ПО УГОЛОВНЫМ ДЕЛАМ

Аннотация. Автор рассматривает возможность перехода на электронный формат уголовного судопроизводства и его влияние на функцию защиты. Утверждается, что дальнейшее развитие получит электронный документооборот, информирование участников уголовного процесса, дистанционный режим осуществления следственных и процессуальных действий, защита данных. Предполагается, что внедрение электронного уголовного дела расширит возможности стороны защиты и сохранит существующие принципы и стандарты уголовного судопроизводства.

Ключевые слова: электронное уголовное дело, функция защиты, реформирование, электронный документооборот

REFORMING THE PROTECTION FUNCTION DURING THE TRANSITION TO THE ELECTRONIC FORMAT OF PROCEEDINGS IN CRIMINAL CASES

Abstract. The author considers the possibility of transition to electronic format of criminal proceedings and how it may affect the defense function. It is stated, that electronic document flow, informing of participants of criminal proceedings, remote execution of investigative and procedural actions, data protection will be developed further. It is anticipated, that implementation of electronic criminal case will broaden opportunities for defense party and preserve existing principles and standards of criminal proceedings.

Keywords: Electronic criminal case, Defense function, Reforming, Electronic document management

В юридической литературе активно обсуждается вопрос о возможном переходе на цифровой формат ведения уголовного судопроизводства. Это влечет такие перспективы, как отказ от бумажных носителей информации, широкое использование электронных документов и дистанционных форм коммуникаций, экономия материальных средств и времени, упрощение и защита данных. Безусловно, электронное уголовное дело – хорошая перспектива развития российского уголовного процесса.

Р. В. Пенез предлагает под этим понимать «электронно-фиксированную информацию, при помощи аппаратно-технических устройств и программных средств, которая выражена в установленном формате, отражающую какой-либо факт или событие, имеющее отношение к уголовному делу и заполняемую соответствующим должностным лицом с целью осуществления расследования по уголовному делу» [5. С. 54].

Н. Е. Борохова к преимуществам производства в электронной форме относит: сокращение сроков ознакомления участниками уголовного судопроизводства с материалами уголовного дела, не будет необходимости согласовывать график ознакомления, возможно, будет выработан стандарт ознакомления с делом, сни-

зится нервозность, улучшится качество подготовки к судебному разбирательству, повысится прозрачность расследования [1. С. 156].

Что же следует ожидать непосредственно для функции защиты в случае перехода на электронный формат производства по уголовным делам?

Прежде всего, это касается электронной формы подачи заявления. Такая форма обсуждается, как правило, применительно к лицу, пострадавшему от преступления. Конечно, это важно, но для стороны защиты не менее принципиально иметь возможность еще на ранних стадиях уголовного процесса подавать в электронном виде свои заявления, жалобы, ходатайства. И это должно распространяться не только на стадии рассмотрения уголовных дел в суде, но и на досудебное производство.

Кроме того, представляется необходимым предусмотреть электронную форму подачи заявления о предоставлении информации о возможном осуществлении уголовного преследования лица путем проведения оперативно-розыскных мероприятий. В основе своей позиции хочется сослаться на решение Конституционного Суда Российской Федерации по делу Черновой И. Г. [6]. Кроме того, согласно ст. 5 Федерального закона «Об оперативно-розыскной деятельности» лицо вправе запросить сведения о полученной в ходе проведения оперативно-розыскных мероприятий информации о нем, а в случае отказа обратиться с жалобой в суд.

Немаловажным для электронного уголовного производства является копирование информации при производстве по уголовном делу. Для стороны защиты это возможность получения материалов уголовного дела в электронном виде. И здесь возможности участников не стоит ограничивать, ограничения устанавливает сам закон в виде тайны предварительного расследования, защиты свидетелей, правил копирования и т. д. В связи с развитием технологий, представляется логичным в случае использования видеозаписи при производстве следственных действий, стороне защиты предоставлять копию технической записи и предоставлять доступ к ее оригиналу неограниченное время. При этом факт копирования должен отражаться в протоколе, а количество сделанных копий с оригинала также фиксироваться в цифровой системе.

По-иному должно осуществляться информирование участников о движении уголовного дела. Возможность ознакомиться с текущем состоянии дел – важная гарантия, позволяющая своевременно реагировать, участвовать и иметь представление о принятых решениях, о сроках, о должностных и иных лицах, имеющих отношение к делу. Информирование может быть посредством смс оповещения, по электронной почте и т. д. в автоматическом режиме. В информировании следует также предусмотреть элемент обратной связи, когда участник уголовного процесса, оповещенный, отвечает в электронном виде о факте получения сведений, а также о готовности прибыть в назначенное время, место и т. д. О причинах, исключающих участие в процессуальных действиях, лицо также должно иметь возможность сообщить об этом посредством сети Интернет. Информирование в бумажном виде следует признать неким анахронизмом.

Электронное уголовное дело невозможно без широкого применения дистанционных форм взаимодействия с применением систем видеоконференцсвязи. Это предполагает развитие уже существующих форм, реализуемых в ходе проведения следственных действий и в ходе судебных заседаний. Обсуждается возможный

переход на видеопротоколирование [4. С. 166]. Не секрет, что показания, данные допрашиваемым лицом могут фрагментарно, а местами значительно отличаться от текста, записанного следователем в протокол. Обвиняемый, потерпевший или свидетель могут иметь относительно скудную речь или невнятно выражать свою мысль. Чтобы лицо, производящее расследование, не имело возможности интерпретировать сказанное субъективно, необходимо сопровождать следственные действия автоматической фиксацией хода и результатов их проведения. Одним из таких решений и может быть внедрение видеопротоколирования [3. С. 7], что позволит избавиться от бумажного делопроизводства.

Электронное производство по уголовным делам должно в корне изменить весь электронный документооборот. Электронное уголовное дело предполагает широкое использование электронных документов. Поэтому понадобится обеспечить всех участников следственных или судебных действий электронной подписью, что придаст легитимность документам и обеспечит выполнение требований закона. Кроме того, цифровая система уголовного судопроизводства должна позволять любому участнику уголовно-процессуальных отношений самостоятельно прикреплять документы в электронном виде. Для стороны защиты это возможность реализовать в какой-то степени так называемое адвокатское расследование, так как откроет дополнительные возможности по сбору и прикреплению к делу доказательств. Это должно происходить независимо от желания лица, производящего расследование, то есть в автономном режиме. Лицо, производящее расследование, должно лишь получить уведомление об этом.

Переход на электронный формат уголовного производства потребует эффективную систему защиты данных. Важный аспект, поскольку требует применения современных технологий и программ защиты сведений в электронном виде. Для стороны защиты представляется важным обеспечить цифровую конфиденциальную видеоконференцсвязь адвоката с подзащитным. Такой канал может иметь самостоятельную функцию, но обязательно анонсироваться (фиксироваться, отражаться) в общем электронном деле. Интерфейс может предусматривать специальную вкладку для подключения данных лиц к видеосвязи.

Расширение возможностей по использованию цифровых технологий в уголовном судопроизводстве не должно повлечь сокращения объема процессуальных гарантий. Внедрение электронного уголовного дела должно расширить возможности стороны защиты по участию в доказывании, а также сохранить существующие принципы уголовного судопроизводства.

Список литературы

1. Борохова Н. Е. Электронное уголовное дело как одно из направлений экологизации уголовного процесса // Университетские правовые диалоги «Право и экология»: материалы Международной научно-практической конференции. 25–26 марта 2021 г. / под ред. Е. В. Титовой. Челябинск, 2001. С. 154–157.

2. Гаврилин Ю. В., Победкин А. В. Модернизация уголовно-процессуальной формы в условиях информационного общества // Труды Академии управления МВД России. 2019. № 3 (51). С. 27–38.

3. Зуев С. В. Цифровое видеопротоколирование следственных действий: возможности и перспективы // Ученые записки: сборник научных трудов. Оренбург, 2020. С. 7–10.

4. Макарова О. В. Совершенствование судопроизводства путем внедрения электронной формы уголовного дела // Журнал российского права. 2019. № 2 (266). С. 159–168.

5. Пенез Р. В. Содержание понятия «электронное уголовное дело» в уголовном судопроизводстве // Право Донецкой Народной Республики. 2018. № 4 (12). С. 42–45.

6. По делу о проверке конституционности отдельных положений Федерального закона «Об оперативно-розыскной деятельности» по жалобе гражданки Черновой И. Г.: определение Конституционного Суда РФ от 14 июля 1998 г. № 86-О // Вестник Конституционного Суда РФ. 1998. № 6. С. 10–27.

Н. В. Карепанов,
кандидат юридических наук,
доцент кафедры криминалистики,
Уральский государственный юридический университет

ОСОБЕННОСТИ ПОИСКА, ИССЛЕДОВАНИЯ И ИСПОЛЬЗОВАНИЯ СЛЕДОВ ПРЕСТУПЛЕНИЙ В КИБЕРПРОСТРАНСТВЕ

Аннотация. Статья посвящена взаимосвязи методологии науки, теории криминалистики с вопросами исследования цифровых технологий, связанных с расследованием преступлений. Природа науки криминалистики, парадигмы теории сегодня подвержены существенным изменениям. Показаны влияние направленности изысканий к потребностям практики, неоднозначный характер подготовки практических рекомендаций, сложный путь фундаментальных исследований до внедрения методов расследования в следственную практику. Специалисты называют пять направлений такого регулирования: защита личных данных и частной жизни в Сети; регулирование электронной коммерции и иных сделок и обеспечение их безопасности; защита интеллектуальной собственности; борьба против противоправного содержания информации и противоправного поведения в Сети; правовое регулирование электронных сообщений.

Ключевые слова: расследование преступлений, цифровая технология, вредоносные программы, антивирусный мониторинг, иммунизация, киберпространство, техническое опережение

SPECIFICS OF THE SEARCH, RESEARCH AND USE OF TRACES OF CRIME IN CYBERSPACE

Abstract. The article focuses on the relationship between the methodology of science, the theory of criminology with the issues of digital research related to the investigation of crimes. The nature of forensic science, the paradigms of theory are now subject to significant changes. The impact of the focus of research on the needs of the practice, the

ambiguous nature of the preparation of practical recommendations, the complex path of fundamental research before the introduction of investigative methods in the investigative practice are shown. The solution to this problem needs to be addressed comprehensively: to study and evaluate the situation in the networks; to implement and balance the forces and means, to ensure cooperation; to manage, plan and control; coordination of actions of law enforcement actors. Forensic. In addition, Internet relationships need to be regulated.

Keywords: Crime investigation, Digital technology, Inbred-bearing programs, Antivirus monitoring, Immunization, Cyberspace, Technical lead

Много вопросов возникает в вопросах теоретического и практического исследования цифровых следов IT-технологий. В настоящее время наблюдается чрезвычайно стремительный прорыв в развитии знаний в области компьютерных и информационных технологий. Использование этих достижений осуществляется разными темпами преступниками и правоохранительными органами. В механизме современных преступлений на постоянной основе стали использоваться информационно-телекоммуникационные технологии и роботизированные системы. Так, в 2018 г. такие технологии и системы использовались с приростом 92,8 % (170 тыс.), в 2019 г. – более 68,5 % (294 тыс.), в 2020 г. – более 77 % (363 тыс.). Увеличился и удельный вес таких преступлений среди других: в 2018 г. – 8,8 %, в 2019 г. – 14,5 %, в 2020 г. – более 23,6 % [2. С. 174–175].

При этом нераскрытыми остаются три четверти этих киберпреступлений. Сказывается хроническое отставание правоохранительных органов в эффективном использовании достижений в области информационных технологий. Конечно, задача их намного сложнее. Они должны не только пользоваться уже готовым, но в большей степени заниматься поиском новых методов установления по цифровым следам компьютерного события и лиц причастных к такому производству. Преодоление создаваемого методического и технического вакуума требует много усилий [1. С. 172].

С 2001 г. в международный обиход входит термин «киберпреступность» [9. С. 185]. В научной зарубежной и отечественной литературе прочно утверждается понятие «цифровая криминалистика» [3. С. 161–171; 8; 10; 11]. Появляются отдельные исследования по разным направлениям цифровых следов: В. А. Мещеряков о месте специальных познаний в цифровой криминалистике; С. Ю. Скобелин об электронных следах преступлений; Н. Н. Федотов о новом направлении компьютерной криминалистики – форензике [5. С. 87–92; 6. С. 178–181; 7].

Современные криминалистические исследования цифровых следов не должны ограничиваться только рамками киберпреступлений. Требуется поиск новых информационных технологических методик для исследования таких следов в целом и использование их для раскрытия преступлений по отдельным перспективным направлениям. Одним из таких направлений можно считать сферу информационно-телекоммуникационных технологий. К актуальным вопросам научных исследований цифровых следов в этой области знаний можно отнести: выявление и описание закономерностей возникновения следов в информационно-телекоммуникационной сфере, включая сеть Интернет; разработка методов диагностики

личности преступника по обнаруживаемым цифровым следам; разработка методов обнаружения и исследования цифровых следов шифрования и анонимизации данных пользователя существующих информационных сетей и используемых технологий; выявление и описание закономерностей возникновения цифровых следов противодействия расследованию преступлений; разработка методов обнаружения и исследования цифровых следов противодействия; разработка теоретических основ методик обнаружения, исследования и использования цифровых следов в информационно-телекоммуникационной сфере. Аналогичную научную работу следует произвести и по иным направлениям исследования цифровых следов [1. С. 173–174].

Большую проблему составляет вопрос разделения знаний профессиональных IT-технологий и криминалистические знания о цифровых следах (их механизм образования, методы обнаружения и исследования). На наш взгляд, это очень тонкая грань и найти параметры принадлежности к той или иной группе знаний – задача будущего. Так, криминалисты часто способны найти улики, которые были удалены из памяти компьютера. Операционные системы удаляют файлы не сразу, а просто прячут их на случай, если то место, которое они занимают, понадобится для чего-то еще. Компьютерные аналитики разработали программы, которые позволяют находить и восстанавливать подобные скрытые. Трудно определить, что входит в компетенцию криминалиста, а что IT-специалиста. Или иногда для выявления следов на компьютере устанавливают кейлогер – программу для перехвата информации, вводимой с клавиатуры. Каждый раз, когда на компьютере печатают или кликают мышкой, кейлогер делает скриншоты (снимок экрана). Но когда скриншотов становится много, кейлогер уничтожает часть из них, чтобы не перегружать жесткий диск. Обычно «Фейсбук» (признана экстремистской организацией, запрещена в РФ) не оставляет следов на жестких дисках. Все происходит в браузере. Однако сам «Фейсбук» сохраняет чаты, даже если их стерли. Это знания какого уровня?

Другое дело, когда следы можно найти и на девайсе (техническое устройство, которое работает от батарейки или розетки, и выполняет различные функции), который часто несет на себе отпечатки пальцев и следы ДНК. Вместе с тем магнитные кисти криминалистов при снятии отпечатков пальцев излучают электромагнитное поле и могут повредить информацию в самом девайсе. Поэтому их помещают в антистатические пластиковые пакеты и неповрежденными передают специалистам по цифровым технологиям (чаще всего, компьютеры, смартфоны и планшеты). Первоначально содержимое девайса всегда копируется, чтобы сохранить оригинал в неприкосновенности. Или можно обратить внимание на информационные следы, заложенные в изображениях и видеофайлах, снятых на цифровые камеры и смартфоны (метаданные). С их помощью можно установить изготовителя, модель камеры, дату и время изготовления снимка и др. Современные девайсы могут быть включены в метаданные GPS-координаты для определения местоположения фотографа. В этих случаях можно смело утверждать о компетенции криминалиста. Но тут опять возникает проблема.

Целый ряд действий выполнить без специальных знаний невозможно. Так, содержимое последних айфонов и блэкберри (смартфон, имеющий возможность

работы с СМС, электронной почтой, позволяющий достаточно удобно просматривать интернет-страницы, а также работающий с другими удаленными сервисами) скопировать практически нельзя. Для доступа к файловой системе нужно снять ограничения (сделать джейлбрейк). Главной целью джейлбрейка является получение полного доступа к файловой системе, а это, в свою очередь, позволяет устанавливать приложения не из App Store, взламывать внутриигровые покупки, менять системные файлы, добавлять темы оформления и новые фишки в iOS. В нынешних айфонах и андроидах их передвижения фиксируются по умолчанию, указывая их местоположение (функцию можно отключить). В смартфоне iPhone 5S есть особый чип геолокации, который работает и на запасном питании (до четырех дней после отключения батарей). При отключении функции определения местоположения возможность определения места через оператора (телефон всегда на связи с сотовыми вышками).

Или, в социальных сетях Интернет типа «Фейсбук» и других при пользовании на смартфонах или планшетах остаются следы, которые фиксируются и могут быть отслежены. Также остаются следы от размещения данных в «облаке», куда зайти можно с любого компьютера. Но с помощью девайсов ее не получить, потому что ее там нет. Существуют технические трудности. Также имеют свои сложности для обнаружения цифровых следов «облачные» вычисления. Сегодня существует возможность синхронизировать файлы между разными компьютерами (переписывать и менять файлы на любом компьютере с любого другого) при помощи сервиса Dropbox или аналогичных ему. Кроме того, в современном мире известны разработки гаджета D-Central, который можно подключить к любому компьютеру, смартфону или планшету и обеспечить приватность общения в Интернете.

Сокрытие цифровых следов или, вернее, сокрытие следов обмена информацией – тоже порождение современности: аналоговые камеры не включают метаданные в фотографии или видеоизображения; доски объявлений можно выставлять и в Интернете; использование старых программ и оборудования, использование мобильного телефона с предоплаченными услугами. Компьютерные данные являются только дополнительными следами, материально фиксированные следы остаются в своей основе. «Отсутствие доказательств не есть доказательство отсутствия» [4. С. 252–259].

Список литературы

1. Каримов В. Х. О развитии системы криминалистического обеспечения борьбы с преступностью в информационно-телекоммуникационной сфере // Отечественная криминалистика: вчера, сегодня, завтра: сб. науч.-практ. Статей / под общ. ред. проф. И. М. Комарова. Москва: Юрлитинформ, 2020. С. 172.

2. Карпов Я. С. О концепции прекурсоров в криминалистике // Отечественная криминалистика: вчера, сегодня, завтра: сб. науч.-практ. статей / под общ. ред. проф. И. М. Комарова. Москва: Юрлитинформ, 2020. С. 174–175.

3. Комаров И. М. «Цифровая» криминалистика – давно назревшая проблема // Библиотека криминалиста. 2018. № 2 (37). С. 161–171.

4. Макдермид В. Анатомия преступления: что могут рассказать насекомые, отпечатки пальцев и ДНК/ пер. с англ. 2-е изд. Москва: Альина нон-фикшн, 2019. 344 с.

5. Мещеряков В. А. Особенности специальных знаний, используемых в цифровой криминалистике // Известия Тульского государственного университета. Экономические и юридические науки. 2013. Т. 4–2. С. 87–92.

6. Скобелин С. Ю. Цифровая криминалистика: понятия, возможности, перспективы // Труды Академии МВД Республики Таджикистан. Материалы республиканской научно-практической конференции с участием международных экспертов «Роль криминалистики в раскрытии и расследовании преступлений» (Душанбе. 25 сентября 2015 г.). С. 178–181.

7. Федотов Н. Н. Форензика – компьютерная криминалистика. Мосвка: Юридический мир, 2007.

8. Яковлев А. Н. Цифровая криминалистика как фактор защиты цифровой экономики. // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): сборник статей Международного науч.-практ. конференции. Москва: Академия управления МВД России. 2018.

9. Convention on Cybercrime Details of Treaty No. 185.

10. Thomas, J., Bossler, M., Kathryn, C. Seigfried-Spellar Cybercrime and Digital Forensics: An Introduction. Routledge, 2nd ed, Berlin, Heidelberg, 2017.

11. Joakim K. Fundamentals of Digital Forensics, Theory, Methods. and Real-Life Applications. Springer International Publishing, Berlin, Heidelberg, 2018.

В. В. Коломинов,
кандидат юридических наук, доцент,
Байкальский государственный университет

НЕКОТОРЫЕ АСПЕКТЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Аннотация. В предложенном материале затрагиваются некоторые проблемы расследования преступлений, сопряженных с использованием криптовалюты. Автор со ссылками на правовую доктрину и материалы судебной практики обозначает криптовалюту в качестве средства и предмета преступления. Далее раскрываются особенности расследования криптопреступлений, связанные с установлением события преступления (времени и места совершения), преодолением разрыва между местонахождением преступника и программно-аппаратных комплексов, а также со спецификой криптовалюты как виртуального средства разрыва между денежными средствами, полученными преступным путем, и предикатным преступлением. Автор обращает внимание на отсутствие некоторых важных элементов в рамках правовой материи, которые необходимы при расследовании преступлений, совершаемых при с использованием криптовалюты. В заключении говорится о том, что разрешение выявленных проблем возможно путем совершенствования нормативной правовой базы, которая станет толчком к выработке валидной правоприменительной, следственной и судебной практики.

Ключевые слова: криптовалюты, блокчейн, криптопреступления, предикатные преступления, расследование преступлений, правоприменительная практика

SOME ASPECTS OF THE INVESTIGATION OF CRIMES COMMITTED USING CRYPTOCURRENCY

Abstract. The proposed material touches upon some problems of investigating crimes involving the use of cryptocurrencies. The author, with references to legal doctrine and materials of judicial practice, designates cryptocurrency as a means and subject of crime. Further, the features of the investigation of cryptocrimes related to the establishment of the crime event (time and place of commission), bridging the gap between the location of the criminal and software and hardware complexes, as well as the specifics of the cryptocurrency as a virtual means of the gap between the funds obtained by criminal means and predicate crime are revealed. The author draws attention to the absence of some important elements within the framework of the legal matter that are necessary in the investigation of crimes committed with the use of cryptocurrencies. The conclusion states that the resolution of the identified problems is possible by improving the regulatory framework, which will be an impetus to the development of valid law enforcement, investigative and judicial practice.

Keywords: Cryptocurrencies, Blockchain, Crypto crimes, Predicate crimes, Crime investigation, Law enforcement practice

Развитие информационно-коммуникационных технологий в условиях постиндустриального общества повлекло за собой возникновение нового способа расчета в форме криптовалюты. Основанная на технологии «блокчейн», криптоиндустрия генерирует особые цифровые денежные единицы, отличные от фидуциарных и фиатных денег, оборот которых регулируется государством и которые, следовательно, обеспечиваются централизованной публичной властью. Криптовалюты, очевидно, удобны при проведении сделок. Тем не менее отсутствие юрисдикционного контроля позволяет использовать криптовалюты для успешного ведения преступной деятельности: торговли оружием, наркотическими средствами и психотропными веществами, финансирования терроризма и распространения оружия массового уничтожения, легализации доходов, полученных преступным путем.

В сущности, сам оборот криптовалюты в Российской Федерации не относится к числу преступных деяний, хотя и легальные расчеты посредством цифровых финансовых активов ограничены. Согласно ст. 75 Конституции Российской Федерации, денежной единицей является рубль, и расчеты в рамках российской правовой системы за исключением использования иностранной валюты в случаях, указанных в Федеральном законе от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле», проводятся в рублях. Тем не менее при совершении некоторых преступлений криптовалюты могут дополнять объективную сторону преступления в качестве средств, т. е. «тех орудий и приспособлений, при помощи которых было совершено преступление» [1. С. 376]. Например, речь может идти о приобретении наркотических средств для дальнейшего сбыта. Предметом преступления в данном случае являются непосредственно вещества, а средством совершения – цифровые финансовые активы, которые способствовали их приобретению. Также крипто-

валюта может являться побочным предметом преступлений, что подтверждается Постановлением Пленума Верховного Суда РФ от 26 февраля 2019 г. № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем», согласно которому предметом преступлений, ответственность за которые наступает по ст. 174–174.1 Уголовного кодекса Российской Федерации, выступают денежные средства, полученные из виртуальных активов, которые, в свою очередь, были получены в результате совершения уголовно наказуемых деяний.

Если говорить непосредственно о расследовании преступлений, связанных с оборотом криптовалют, то необходимо обратить внимание на следующие обстоятельства. Во-первых, надлежит установить событие преступления, в рамках которого средством или предметом выступает криптовалюта. Для заключения о событии следует выявить место и время совершения преступления с использованием цифровых активов. Сложность данной задачи заключается в том, что программно-аппаратные комплексы для получения криптовалют могут не совпадать с фактическим местонахождением лица, совершающего преступное деяние. При выявлении времени совершения преступления также возникают очевидные трудности, объясняемые тем, что «разнообразные подсистемы компьютера время того или иного события фиксируют в разных часовых поясах и разной кодировке» [2. С. 226].

Также очевидные трудности расследования преступлений, совершенных с использованием криптовалюты, обуславливаются самой спецификой криптовалюты как виртуального актива, который напрямую не может выйти в мир реальный. Учет такой специфики особенно важен при расследовании преступлений, связанных с легализацией преступных доходов. Как справедливо заметили И. М. Середа и С. А. Ступина, «в связи с переходом из физического в виртуальный мир, биткоин потенциально способен разрушить все связи между незаконными доходами и предполагаемым преступлением», поскольку «этот переход непоправимо разрывает все связи между замещаемым имуществом и предикатным преступлением» [3. С. 90].

Кроме всего прочего, считаем важным обратить внимание на отсутствие следующих важных элементов в рамках правовой материи, которые необходимы при расследовании преступлений, совершаемых при с использованием криптовалюты: развитой нормативной правовой базы в сфере регулирования криптовалюты и цифровых финансовых активов, методического аппарата, способствующего раскрытию криптопреступлений, разветвленной судебной и следственной практики в сфере криптопреступности, необходимой практической подготовки у сотрудников правоохранительных органов, занимающихся расследованием преступлений, совершаемых с использованием криптовалюты.

В завершение материала заметим, что разрешение поднятых нами проблем находится в правовой и практической плоскостях. Посредством принятия специальных правовых актов об обороте криптовалюты появится ясность относительно юридического статуса цифровых финансовых активов в уголовно-правовых отношениях, что, в свою очередь, станет толчком к наработке четкой и позитивной следственной, правоприменительной и судебной практике.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) // Российская газета. 25 декабря 1993 г. № 237.
2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 17 июня 1996 г. № 25. Ст. 2954.
3. Федеральный закон «О валютном регулировании и валютном контроле» от 10.12.2003 № 173-ФЗ // Собрание законодательства Российской Федерации. 15 декабря 2003 г. № 50. Ст. 4859.
4. Постановление Пленума Верховного Суда РФ от 26 февраля 2019 г. № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // Бюллетень Верховного Суда Российской Федерации. Апрель 2019 г. № 4.
5. Наумов А. В. Российское уголовное право. Общая часть. Курс лекций. Москва: Проспект, 2017. 784 с.
6. Надысева Э. Х. Проблемы расследования преступлений в сфере оборота криптовалют // Вестник экономической безопасности. 2019. № 3. С. 223–227.
7. Середа И. М., Ступина С. А. Потенциал уголовного законодательства в сфере противодействия преступлениям, связанным с криптовалютой // Пролог: журнал о праве. 2021. № 4. С. 85–96.

М. Н. Кузбагаров,
кандидат юридических наук, доцент,
Санкт-Петербургский государственный экономический университет;
Северо-Западный институт управления Российской академии
народного хозяйства и государственной службы
при Президенте Российской Федерации
Е. В. Кузбагарова,
кандидат юридических наук, доцент,
Санкт-Петербургский государственный
архитектурно-строительный университет
Т. Б. Дондукова,
кандидат юридических наук, доцент,
Санкт-Петербургский государственный
архитектурно-строительный университет

СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА БЛОКЧЕЙН-ТЕХНОЛОГИЙ

Аннотация. В статье рассматриваются понятийные, правовые, организационные аспекты производства судебной компьютерно-технической экспертизы (далее – СКТЭ) блокчейн-технологий при осуществлении судопроизводства. Авторами исследуется этимология понятия «блокчейн» технологий, определяется сфера их

применения и необходимость на законодательном уровне урегулирования процедуры осуществления судебной компьютерно-технической экспертизы блокчейн-технологий. Затрагивается вопрос использования блокчейн-технологий в судебной экспертизе в качестве инструментария хранения данных. Уделяется внимание специфике производства СКТЭ операций, осуществляемых с криптовалютой.

Ключевые слова: судебная компьютерно-техническая экспертиза, блокчейн, криптовалюта, криптокошелек, расследование

JUDICIAL COMPUTER AND TECHNICAL EXAMINATION OF BLOCKCHAIN TECHNOLOGIES

Abstract. The article discusses the conceptual, legal, organizational aspects of the judicial computer-technical expertise of blockchain technologies in the implementation of legal proceedings. The authors investigate the etymology of the concept of "blockchain" technologies, determine the scope of their application and the need at the legislative level to regulate the procedure for the implementation of forensic computer-technical expertise of blockchain technologies. The issue of using blockchain technologies in forensic examination as a data storage tool is touched upon. Attention is paid to the specifics of the production of forensic computer-technical expertise of operations carried out with cryptocurrency.

Keywords: Forensic computer forensics, Blockchain, Cryptocurrency, Crypto wallet, Investigation

Современный мир развивается в эпоху цифровых, информационных технологий, которые из года в год непрерывно совершенствуются. С геометрической прогрессией растет число пользователей сети Интернет, происходит всеобщая киберинтеграция. Компьютерные технологии охватили основные сферы деятельности: политика, судопроизводство, экономика, гос. управление, менеджмент, образование, бизнес и наука. Практически все перешло в виртуальный мир: общение, образование, покупки, банковские транзакции, хранение информации и прочее. Одну из ведущих ролей в данных процессах занимает блокчейн-технологии в различных ее проявлениях.

Для того чтобы выяснить влияние блокчейн-технологий на компьютерно-техническую экспертизу (далее по тексту – СКТЭ), в начале нужно понять, что такое блокчейн, определить его особенности и недостатки, сферу использования. Ведь не только лишь одна из особенностей или не один из видов технологии блокчейн оказывают влияние на СКТЭ, а именно его комплексные особенности и функции, то есть все вместе взятые.

Без сомнений можно сказать, что блокчейн является революционным явлением современного мира. Мир узнал о блокчейне благодаря созданию новой цифровой криптовалюты Bitcoin. В 2008 г. в статье «Bitcoin: A Peer-to-Peer Electronic Cash System» понятие «блокчейн» было впервые использовано автором Сатоши Накамото. В документе Сатоши Накамото описывает основы криптовалюты биткоин, что и легко в основу блокчейна [7].

Блокчейн – это «распределенная база данных, которая состоит из «цепочки блоков» устройства хранения блоков не подключены к общему серверу, база данных позволяет контролировать достоверность транзакций без надзора каких-либо финансовых устройств». Таким образом, блокчейн представляет собой технологию распределенного реестра. Вся цепочка операций и список владельцев хранится на многих компьютерах независимых пользователей. В случае если произойдет сбой одного или нескольких компьютеров, то информация не пропадет из всей цепочки, а сохранится у других пользователей [6. С. 41].

Блокчейн – это инновационная технология, которая обладает важнейшими факторами: безопасностью, эффективностью, прозрачностью, уменьшает риск с третьими лицами, сокращает время на обработку транзакции, является, бесспорно, надежной и невероятно функциональной системой.

В 2018 г. российский суд впервые применил блокчейн в системе учета интеллектуальной собственности путем размещения транзакций об изменении состава правообладателей в блокчейн сети IPChain.

Блокчейн-технологии были разработаны с целью управления активами, без посредников при совершении сделок в сети Интернет. В данном случае идентифицировать пользователя приравнивается к процедуре регистрации в реестре по определенному имени, объявленному самим пользователем. При отождествлении идентификатора и субъекта существует такая процедура доступа к данным системы, как аутентификация. Три важных, если не сказать обязательных, элемента доказательства права собственности на объекты, оборот которых происходит в сети Интернет – идентификация, аутентификация и авторизация пользователя. Ввиду роста влияния блокчейн-технологий на правоотношения в области активов подобное разделение не может быть игнорировано юридической наукой. Поэтому можно говорить о том, что идентификация в экспертном смысле охватывает как идентификацию в компьютерно-техническом смысле, так и его аутентификацию.

Для судебного эксперта важно постоянно развиваться и идти в ногу со всеми технологиями современности и первоочередной задачей для него является понимание и способность разбираться во всех передовых технологиях, а также науках, способствующих в достижении поставленных целей. Ведь именно перед данными субъектами судами ставится огромное количество вопросов.

Г. Г. Камалова отмечает, что «алгоритм автоматизированного и автоматического исследования должен быть для эксперта и специалиста максимально прозрачен, поэтому предпочтительными выглядят системы, построенные по принципу “белого ящика”» [1. С. 183]. Блокчейн-технологии как раз являются достаточно прозрачными, позволяющие получать информацию одновременно с нескольких источников ее хранения и путем сопоставления проверить ее идентичность и достоверность в рамках СКТЭ. Аналогичная ситуация складывается и при производстве судебной экономической экспертизы в отношении операций, совершаемых с активами, созданными на основе блокчейн-технологий, в силу того, что ведение регистров бухгалтерского учета данных активов будет осуществляться на нескольких цифровых платформах одновременно и параллельно.

Блокчейн-технологии могут выступать не только в качестве объекта исследования СКТЭ, но и в качестве самостоятельного инструмента хранения данных, фигурирующих в судебных экспертизах. Использование блокчейн-технологий в судебной экспертизе позволит достигнуть высокую степень их надежности и достоверности, так как данная информация будет храниться во взаимосвязанных блоках, синхронизированных между собой по времени, и одновременно храниться на нескольких компьютерах, позволяя исключить возможность несанкционированной модификации информации.

Действительно на данный момент инновационная технология блокчейн развивается в различных сферах: медицине, торговле, транспорте, государственном управлении, финансовой области и т. д.

Безусловно, главная сфера использования технологии блокчейн – криптовалюта [3. С. 214]. В связи с этим на сегодняшний день причины обращения граждан за защитой своих нарушенных прав в сфере использования критовалюты могут быть самыми различными: взлом онлайн-кошелька, похищение криптовалют при взломе личного кабинета на криптовалютной бирже с последующим переводом средств на счет похитителя и др. В свете данных явления актуальным является разработка методики расследования преступлений, связанных с оборотом криптовалюты и использованием в процессе расследования специальных знаний в сфере компьютерных технологий.

А. А. Несмеянов разделяет мнение Э. Х. Надысевой, указывая на то, что в ходе расследования преступлений в области использования криптовалюты наиболее объективная и значимая это информационно-компьютерная экспертиза так как позволяет, в том числе определить транзакции.

Мы разделяем мнение вышеуказанных авторов, что информационно-компьютерная экспертиза как вид СКТЭ помогает решаться вопросы, связанные с восстановлением утерянных документов с электронных устройств, в которых размещались «кошельки» с криптовалютами. Однако стоит отметить, что ввиду отсутствия четкого регулирования в нормативно-правовых актах, установление указанных выше фактов, посредством производства судебной экспертизы, не всегда возможно и, к сожалению, не всегда востребовано.

Таким образом, с ростом блокчейн-технологий, на законодательном уровне должно быть регулироваться и осуществление судебной компьютерно- технической экспертизы таких «объектов».

Одной из актуальных задач экспертов является установление связи между пользователем и его криптокошельком. Ввиду широкого распространения криптовалют и отсутствия обширной судебной практики в данной отрасли, им приходится обращаться, например, к практике арбитражных судов [5].

При регистрации криптокошелька установление личности пользователя аналогично, как и при открытии банковского счета.

В случае оспаривания права собственности на криптовалюту, то выбор средств доказывания права владения криптовалютой может вытекать как из непосредственного исследования средств управления (интерфейса) криптокошелька и его отнесения к какому-либо виду и типу, так и из использования косвенных методов, позволяющих выявление объективной связи между владельцем (пользователем) и криптокошельком.

Это может быть, например, сличение публичного ключа или цифрового идентификатора криптокошелька, размещенного на сайте должника, и идентификатора криптокошелька на бумажном или цифровом носителе, представленном эксперту в качестве материала для исследования. Идентичность публичных ключей будет однозначно подтверждать, что это один и тот же криптокошелек, и с высокой степенью вероятности указывать на то, что пользователем криптокошелька на сайте и криптокошелька для проведения экспертизы, является одно и то же лицо [2].

Однако только факт принадлежности публичного ключа конкретному пользователю не может позволить эксперту сформировать категорический вывод и привести его в заключении. Это возможно, но исключительно в том случае, если заданный эксперту вопрос прямо касается этой принадлежности.

Особые свойства и качества криптовалюты, безусловно, требуют разработки адаптированной к цифровым активам научно-практической основы для проведения экспертных исследований. Однако необходимо признать, что существующие средства и методы судебной экспертизы также позволяют достигать положительных результатов, поскольку общие экономические закон и принципы оборота экономических ценностей остались неизменными.

Следует отметить то, что основные особенности блокчейн-технологии, характеризуется как инновационная технология, которая обладает важнейшими факторами – безопасностью, эффективностью, прозрачностью, и позволяет снизить риски при заключении договоров с третьими лицами, сокращает время на обработку транзакции, является, бесспорно, надежной и невероятно функциональной системой. Однако, несмотря на обилие преимуществ, для успешного внедрения технологии блокчейн необходимо преодолеть ряд сложностей, решить проблемы, которые могут поставить под сомнение данную инновацию.

В рамках рассмотрения данной проблематики следует сделать вывод о том, что блокчейн-технологии используются и внедряются во многие сферы современного мира, и выгода от их применения остается неизменной. Судебная экспертиза не стала исключением из данной тенденции, однако на настоящий момент отсутствует единые экспертные методики производства судебных экспертиз блокчейн-технологий. Сложности экспертного исследования блокчейн-технологий обусловлены отсутствием правовой регламентации понятийного аппарата, признаков и иных элементов блокчейн и регламентированного механизма его использования на территории России. В связи с этим повышение эффективности производства судебной экспертизы блокчейн технологий, в том числе СКТЭ, возможно путем оптимизации законодательства на основе научных выводов.

Список литературы

1. Камалова Г. Г. Цифровые технологии в судебной экспертизе: Проблемы правового регулирования и организации применения // Экономика и право. Вестник Удмуртского университета. 2019. С. 180–186.

2. Кошелек для криптовалюты – как его создать и какой лучше: холодный, мультивалютный, аппаратный или онлайн-криптокошелек. URL: https://ktonanovenkogo.ru/.html (дата обращения: 19.08.2022).

3. Кузбагаров М. Н., Кузбагарова, Е. В. К вопросу о правовом регулировании криптографических систем и их производных в России по состоянию на 2018 год // Новеллы права и политики 2018. 2019. С. 211–216.

4. Несмеянов А. А. Проведение экспертных исследований при расследовании преступлений, связанных с использованием криптовалют // Научный дайджест Восточно-Сибирского института МВД России. 2021. № 4 (14). С. 116–124.

5. Постановление Девятого Арбитражного апелляционного суда от 15 мая 2018 г. № 09АП-16416/2018. URL: http://ivo.garant.ru/#/document/61623374/paragraph/1:0 (дата обращения: 15.08.2022).

6. Федотова В. В., Емельянов Б. Г., Типнер Л. М. Понятие блокчейн и возможности его использования // European Science. 2018. № 1 (33). С. 40–48.

7. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://www.coindesk.com/bitcoin-peer-to-peer-electronic-cash-system (дата обращения: 15.08.2022).

Е. А. Купряшина,
кандидат юридических наук, доцент,
Белгородский государственный национальный
исследовательский университет
М. А. Черепанов,
студент,
Белгородский государственный национальный
исследовательский университет

ЦИФРОВИЗАЦИЯ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Аннотация. В данной научной статье рассматривается актуальность цифровизации процесса уголовного судопроизводства в Российской Федерации. Авторами работы исследуются те решения в области цифровизации уголовного судопроизводства, которые имеют место быть в настоящее время, а также вкупе с этим исследуются перспективы нововведений в уголовно-процессуальном законодательства Российской Федерации. Обоснованы актуальность научного исследования, основные понятия, проводится сравнительный анализ зарубежного опыта цифровизации уголовного судопроизводства.

Ключевые слова: Уголовно-процессуальный кодекс РФ, электронный документ, электронный документооборот, современные технологии, цифровизация, уголовно-процессуальное законодательство, электронное уголовное дело

DIGITALIZATION OF CRIMINAL PROCEEDINGS

Abstract. This scientific work examines the relevance of digitalization of the criminal justice process in the Russian Federation. The authors of the work investigate the solutions in the field of digitalization of criminal proceedings that are taking place at the present time, as well as, together with this, the prospects for innovations in the Criminal Procedure legislation of the Russian Federation are explored. The relevance of

scientific research, basic concepts are substantiated, a comparative analysis of foreign experience of digitalization of criminal proceedings is carried out.

Keywords: Criminal procedure code of the Russian Federation, Electronic document, Electronic document management, Modern technologies, Digitalization, criminal procedure legislation, Electronic criminal case

Процесс научно-технического развития есть ничто иное, как стремительное развитие науки и, соответственно, техники и основополагающих технологических, информационных процессов в развитых странах. Сама по себе деятельность, связанная с научно-техническим прогрессом объективна, постоянно действует во времени и ставит перед обществом и государством, в частности, вопрос о том, что сегодня необходимо неуклонно, и повсеместно соответствовать актуальным технологическим запросам. Синергия запросов общества и целей научно-технического прогресса должна прийти в такой баланс, при котором все актуальные решения будут приниматься на государственном и техническом уровне вовремя и в соответствии с актуальным научно-техническим развитием.

В этой связи стоит отметить точку отсчета, от которой современная эпоха стала непрерывно, а порой даже и стремительно переходить в новую эпоху – эпоху промышленной революции. Данный период истории открывает для научно-технических, информационных обществ важный фактор, без которого нормальная деятельность научно-технического процесса невозможна – это слияние научного и технического процесса. Научные изыскания становятся ничем иным, как основополагающей производственной силой, двигателем открытий, развития знаний. Как итог вышеупомянутого объективного и стремительного процесса – переход общества к инфраструктурной информационно-технологической трансформации, что приводит нас к качественно-инновационному развитию структур общества и государственности. Как итог – переход в так называемую темпорально новую информационную эру, или информационную эпоху. Справедливо отметить, что как и у любого решения, здесь наличествуют две стороны: позитивные и негативные [7. С. 20–29]. В данной научной статье мы затронем позитивные научные тенденции с перспективой развития, а также сравним цифровизацию уголовного судопроизводства с опытом других стран.

Обращаясь к теме цифровизации как таковой в Российской Федерации отметим, что специалисты в области исследования информационных технологий в уголовном судопроизводстве полагают, в частности, одним из результатов подобных инноваций создание так называемого электронного уголовного дела как части комплексной информационно-судебной системы [1. С. 6–12].

Сам по себе процесс цифровизации уголовного судопроизводства, как перспективное направление, должен сперва пройти стадию планирования, затем стадию тестирования, корректировок, результативных оценок, и уже в последствии, перейти к процессу оформления на законодательном и технологическом уровне. Здесь важно при создании подобной системы не нарушить основополагающие принципы УПК РФ, закрепленные в главе 2 «Принципы уголовного судопроизводства» [6].

В этой же связи необходимо отметить, что цифровизация уголовного судопроизводства должна быть направлена не на замену самого уголовно-процессуального

института, на некий его информационный и виртуальный аналог. Подобная инновация должна наоборот, ускорить порядок судопроизводства, создать возможность для оперативного, своевременного, «онлайн» доступа к документам у участников уголовного процесса. Должен реализовываться весь необходимый набор прав и обязанностей в таком же качестве, в таком же смысле, как и в привычной для нас форме уголовного судопроизводства. Сам по себе процесс электронного уголовного процесса может в перспективе избавить правоохранительные органы от таких громоздких и подчас затратных мероприятий, как формирование описей уголовного дела с сопутствующей нумерацией каждого тома уголовного дела. А в связи с данной мыслью нужно отметить, что уголовные дела вполне могут достигать и несколько десятков томов, что вполне себе норма для следователей. Также это избавляет следователя или дознавателя от необходимости работать с исключительно бумажным источником уголовного судопроизводства, в особенности если требуются какие-либо выездные консультации или ознакомление с материалами уголовного дела. Наличие информационной автоматической справочно-уголовной системы позволит исключить оперирование большим количеством бумажных источников, и свести все к современным и технологическим процессам на уровне зарекомендовавшей себя на сегодняшний день системы портала «Государственные услуги». Это один из самых демонстративных примеров того, как технологии способны упростить доступ населения к необходимому документообороту с возможностью формировать заявки на получение различных справок, отчетов, выписок, избавляя обратившегося гражданина от необходимости совершать лишние бюрократические действия.

Другим не менее актуальным примером, нашедшим применение в поле правовой цифровизации, это Единая информационная система нотариата, функционирующая в целях комплексной автоматизации сбора, обработки, использования видов информационного обмена и взаимодействия. Нотариальные данные зачастую используются в уголовном процессе. Централизованным органом управления данной системой является Федеральная нотариальная палата [2]. По статистике, с периода начала 2018 года практически сто процентов нотариальных действий фиксируются именно в электронном виде, облекаясь в юридически правильную форму в рамках Единой информационной системы нотариата, при этом не создавая прецедента для ограничения какой-либо стороны правовых отношений в своих правах или обязанностях.

Среди приведенных примеров достаточно успешно цифровизации документооборота, хотелось бы упомянуть про правовую инициативу республики Казахстан, основанной на изменениях основных положений Уголовно-процессуального закона [5] в период времени с 2017 г. [3]. В связи с проводимой реформой в области цифровизации, начатой еще в 2011 г., властям Казахстана удалось создать собственную систему, позволяющую как регистрировать сообщения о преступлении в информационно-правовой системе, так и осуществлять расследование уголовных дел в электронной форме.

Конкретизируя некоторые положения УПК Республики Казахстан, отметим, что данный нормативно-правовой акт содержит конкретизированное понятие электронного документа, что исключает двойственность трактовок и какие-либо

несостыковки в ходе расследования уголовных дел, а также исключает возможность ошибочной регистрации в реестре электронных уголовных документов. Помимо установленных признаков электронного документа, УПК РК уточняет, что все электронные уголовно-процессуальные документы заверяются цифровой подписью – п. 15 ст. 7 УПК Республики Казахстан.

В целом исключительно подробно уголовно-цифровой порядок судопроизводства конкретно не регламентирован, однако же существующие в настоящее время положения УПК Республики Казахстан, а также актуальный НПА в виде инструкции о ведении уголовного судопроизводства от 3 января 2018 г. указывает на некие пределы возможностей цифровизации уголовного судопроизводства. На основании вышеупомянутого закона от 3 января 2018 г. генеральный прокурор получает дополнительные полномочия принимать нормативные акты, обязательные к исполнению правоохранительными органами в информационно-цифровой форме, – ч. 6 ст. 58 УПК Республики Казахстан.

Функционал «Единого реестра досудебных расследования» (далее – ИС ЕРДР) позволяет в полной мере обеспечить доступ участвующих лиц к электронному документообороту по конкретному уголовному делу после соответствующих процессов авторизации и подтверждения личности со стороны системы регистрации пользователей ИС ЕРДР. Соответственно, то или иное уполномоченное лицо, участвующее в уголовном судопроизводстве, может обеспечивать доступ иным лицам, имеющим на это соответствующее право после необходимой идентификации и регистрации. Стоит отметить, что если на каком-то этапе судопроизводства возникает необходимость перейти на бумажный формат судопроизводства, следователь или иное должностное лицо имеет право поменять формат на бумажный, при наличии мотивированного постановления и каких-либо препятствующих факторов, не позволяющих продолжать уголовное судопроизводства в электронном формате.

При осуществлении деятельности ИС ЕРДР в то же время не отпадает необходимость в бумажных носителях сведений, относимых к конкретному уголовному делу, так как существуют законные положения, при которых осуществление уголовного судопроизводства возможно в бумажной форме: передаче материалов уголовного дела в иностранный орган уголовного судопроизводства, наличие в материалах информации, охраняемой законом (государственная тайна) и др.

Практика применения модуля «электронного уголовного дела» подтверждает, что электронный формат уголовного судопроизводства – это практическое цифровое решение, которое направлено на реализацию задач по укреплению защиты прав человека в уголовном процессе, повышению состязательности сторон и обеспечению прозрачности уголовного процесса.

Таким образом, формирование подобной законодательной инициативы, возможно, создаст прецедент успешной, актуальной и подтвердившей свою полезность и актуальность новеллы в цифровизации современных процессов в обществе. На основании анализа положений УПК Республики Казахстан возможно создать аналогичную систему в органах уголовного правосудия на территории Российской Федерации, реализуя здесь полное обеспечение прав

всех участников процесса на ознакомление с материалами дела, снимая с них необходимость отвлекать следственные органы от основной работы, а также не тратя и свое время на разъезды.

Также при создании оперативного слияния автоматизированной базы данных уголовно-процессуальных документов с техникой следователя, возможно упростить и в то же время обеспечить сохранность всех материалов уголовных дел. Согласно заявлению Генеральной прокуратуры Российской Федерации, в период времени 2015 г. при анализе положения дел в правоохранительных органах РФ было установлено, что не удалось определить судьбу практически 270 тыс. уголовных дел, поскольку на момент формирования отчета все они были утеряны и не восстановлены [4]. Функционирование виртуальной автоматизированной базы хранения документов уголовного судопроизводства позволит исключить потерю документов, также не позволит вносить в них какой-либо подлог в виде подчисток, дописок, травления или иных механических, а также химических способов фальсификации документов.

Список литературы

1. Зуев С. В. Электронное уголовное дело: за и против // Правопорядок: история, теория, практика. 2018. № 4 (19). С. 6–12.

2. Основы законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 № 4462–1) (ред. от 14.07.2022) // Российская газета. № 49. 13.03.1993.

3. О внесении изменении и дополнений в некоторые законодательные акты Республики Казахстан по вопросам модернизации процессуальных основ правоохранительной деятельности: Закон Республики Казахстан от 21 декабря 2017 г. № 118-VI ЗРК // Информационно-правовая система нормативных правовых актов Республики Казахстан. URL: http://adilet.zan.kz/rus (дата обращения: 11.09.2022).

4. Прокуроры выявили 270 тыс. пропавших уголовных дел. URL: https://rg.ru/2015/07/28/prokurori.html (дата обращения: 11.09.2022).

5. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 12.07.2018) // Информационно-правовая система нормативных правовых актов Республики Казахстан. URL: http:// adilet.zan.kz/rus (дата обращения: 11.09.2022).

6. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 14.07.2022, с изм. от 18.07.2022) (с изм. и доп., вступ. в силу с 25.07.2022) // Российская газета. № 249. 22.12.2001.

7. Шестакова И. Г. Новая темпоральность цифровой цивилизации: будущее уже наступило Архивная копия от 27 февраля 2020 на Wayback Machine // Научно-технические ведомости СПбГПУ. Гуманитарные и общественные науки. 2019. № 2. С. 20–29.

С. М. Курбатова,
кандидат юридических наук, доцент,
Красноярский государственный аграрный университет

ИСПОЛЬЗОВАНИЕ ВКС В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ КАК ГАРАНТИЯ РЕАЛИЗАЦИИ ПРАВ ЕГО УЧАСТНИКОВ ИЗ ЧИСЛА ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

Аннотация. В статье обращается внимание на необходимость учета особенностей участников уголовного судопроизводства из числа категорий населения, имеющих ограниченные возможности. Отмечается роль и значение цифровых и иных технологий для реализации прав и исполнения обязанностей участниками правоотношений, имеющих физические и когнитивные ограниченные возможности. Рассматривается вопрос использования ВКС в уголовном судопроизводстве при производстве процессуальных действий как гарантия обеспечения прав их участников из числа лиц с ограниченными возможностями.

Ключевые слова: уголовное судопроизводство, участники уголовного судопроизводства, лицо с ограниченными возможностями, технологии, видеоконференцсвязь, правовой статус, гарантии

THE USE OF VIDEO CONFERENCING IN CRIMINAL PROCEEDINGS AS A GUARANTEE OF THE RIGHTS OF ITS PARTICIPANTS FROM AMONG PERSONS WITH DISABILITIES

Abstract. Attention is drawn to the need to take into account the characteristics of participants in criminal proceedings from among the categories of the population with disabilities. The role and importance of digital and other technologies for the realization of rights and performance of duties by participants in legal relations with physical and cognitive disabilities is noted. The issue of the use of videoconferencing in criminal proceedings in the production of legal proceedings is considered as a guarantee of ensuring the rights of their participants from among persons with disabilities.

Keywords: Criminal proceedings, Participants in criminal proceedings, Persons with disabilities, Technology, Video conferencing, Legal status, Guarantees

Введение. Вопросы, связанные с необходимостью цифровизации уголовного судопроизводства, поднимаются в последние годы все более активно [1, 3, 4]. Одним из направлений в их обсуждении является вопрос по поводу применения результатов науки и техники для содействия обеспечения реализации участниками уголовного судопроизводства своих прав и обязанностей. Более того, применение высоких технологий в уголовном судопроизводстве можно рассмотреть и в качестве гарантии реализации правового статуса его участникам, которые относятся к категории «лица, имеющие ограниченные возможности». И если обратиться к нормам действующего уголовно-процессуального законодательства, то в качестве такой технологии можно назвать предусмотренную Уголовно-процессуальным кодексом РФ (далее – УПК РФ) возможность применять видеоконференцсвязь (ВКС)

для производства следственных и судебных действий, основанных на получении показаний от их участников.

Основная часть. Возможность использования судом, рассматривающим уголовное дело, систем видеоконференцсвязи для проведения допроса свидетеля была предусмотрена Федеральным законом от 20.03.2011 № 39-ФЗ, дополнившим УПК РФ ст. 278.1 «Особенности допроса свидетеля путем использования систем видеоконференцсвязи». Однако в досудебном производстве похожая норма появилась в конце 2021 г., когда Федеральный закон от 30.12.2021 № 501-ФЗ ввел в УПК РФ ст. 189.1 «Особенности проведения допроса, очной ставки, опознания путем использования систем видеоконференцсвязи».

Не вдаваясь в дискуссии по поводу соотношения содержания данных норм, предложений по расширению процессуальных действий, на которые они должны распространяться, трудностей правоприменения, связанных с организацией проведения сессии ВКС, и пр. [2, 5, 6], отметим значимость данной технологии как гарантии реализации правового статуса участников уголовного судопроизводства, из числа лиц, имеющих ограниченные возможности.

Речь идет о таких участниках производства по уголовному делу, которые, при наличии у них затруднений физического характера (отсутствие конечностей, тяжелая болезнь, заболевания опорно-двигательного аппарата и т. п.) и (или) когнитивных, не ставящих под сомнение их дееспособность (жертвы сексуального насилия, несовершеннолетние, запуганные и пр.) не способны в официальной обстановке кабинета следователя или зала судебного заседания надлежащим образом реализовать свои процессуальные права и исполнить обязанности.

Например, в Великобритании еще в 1999 г. был принят Закон о правосудии в отношении молодежи и доказательствах [7], согласно которому предусматривалось предоставление некоторым категориям лиц ряда специальных мер для обеспечения их надлежащего участия. В числе данных мер была и возможность дачи показаний удаленно, по ВКС; а к таким лицам были отнесены участники:

– которым не исполнилось 18 лет на момент слушания ходатайства о применении специальных мер или которыми были представлены свои доказательства, записанные ими на видео, в возрасте до 18 лет, хотя бы им исполнилось 18 лет до суда;

– качество показаний которых, вероятно, будет снижено из-за наличия: физической инвалидности или физического расстройства; значительного ухудшения интеллекта и социального функционирования; психического расстройства [8].

Подобные правовые нормы с начала XXI в. стали активно появляться и во многих других странах англо-саксонской правовой семьи (США, Канада, Австралия, Новая Зеландия и др.) и продолжают действовать и по настоящее время, лишь дополняясь и совершенствуясь. с учетом практики их применения, а также развития цифровых, информационных и иных технологий.

Заключение. Расширение границ использования технологий в уголовном судопроизводстве в нормах российского уголовно-процессуального законодательства будет направлено на содействие обеспечению надлежащего участия в нем лиц с ограниченными возможностями, в случае их привлечения в качестве его участников. Об этом свидетельствуют как положительный опыт применения технологий для процессов

реабилитации, адаптации и пр., направленных на максимальную компенсацию тех возможностей, которые ограниченны в результате болезней, психологических травм и т. д., так и успешный пример законодательного их введения и использования непосредственно в уголовном судопроизводстве в ряде иностранных государств.

Список литературы

1. Бертовский Л. В. Цифровое судопроизводство: проблемы становления // Проблемы применения уголовного и уголовно-процессуального законодательства: сборник материалов международной научно-практической конференции. Симферополь: типография «Ариал», 2018. С. 173–178.

2. Бодяков В. Н., Морозов Р. М. Актуальные вопросы внедрения института производства отдельных следственных действий, проводимых дистанционно с использованием видеоконференцсвязи в местах лишения свободы // Вестник Кузбасского института. 2021. № 2 (47). С. 115–131.

3. Воскобитова Л. А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex russica (Русский закон). 2019. № 5. С. 91–104.

4. Григорьев В. Н., Суходолов А. П., Ованесян С. С. и др. Цифровые информационные платформы как предмет нормативно-правового регулирования в сфере уголовного судопроизводства // Всероссийский криминологический журнал. 2019. Т. 13, № 6. С. 873–883.

5. Овчинникова О. В. Дистанционные следственные действия: современное состояние и перспективы // Юридическая наука и правоохранительная практика. 2019. № 1 (47). С. 108–116.

6. Плетникова М. С., Семенов Е. А. К вопросу использования видеоконференцсвязи при производстве допроса // Уральский юридический институт МВД России. № 1 (29). 2021. С. 25–28.

7. Youth Justice and Criminal Evidence Act 1999. URL: https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/101874/122971/F869309176/GBR 101874.pdf (дата обращения: 16.09.2022).

8. Victims and Witnesses. Vulnerable or intimidated witnesses. URL: https://www.ppsni.gov.uk/vulnerable-or-intimidated-witnesses (дата обращения: 16.09.2022).

Е. А. Лаврушко,
магистр юридических наук, преподаватель,
Казахско-русский международный университет

ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ В УГОЛОВНОМ ПРОЦЕССЕ

Аннотация. В данной статье рассматриваются основные аспекты и дальнейшие перспективы развития и перехода к использованию современных цифровых технологий. В современном мире невозможно представить большинство протекаемых процессов и общественных отношений без помощи информационных ресурсов. Наиболее актуальным в настоящее время, по мнению ученых и экс-

пертов-практиков, является вопрос проблемы применения современных цифровых технологий в сфере правовых отношений и в уголовном процессе. Переход к приоритету использования цифровых источников имеет свои как достоинства, так и недостатки. Наличие недостатков обусловлено несовершенством технического оснащения, не всегда эффективная, качественная и стабильная работа сети Интернет. К преимуществам в первую очередь можно отнести удобство применения, сокращение времени, а также свободный доступ при получении государственных услуг гражданами.

Ключевые слова: цифровые технологии, государство, интернет-ресурсы, цифровизация, интернет-мошенничество, программа, следствие, уголовный процесс

LEGAL ASPECTS OF THE USE OF MODERN DIGITAL TECHNOLOGIES IN CRIMINAL PROCEEDINGS

Abstract. This article discusses the main aspects and further prospects of development and transition to the use of modern digital technologies. In the modern world, it is impossible to imagine most of the ongoing processes and public relations without the help of information resources. The most relevant issue at present, according to scientists and expert practitioners, is the problem of the use of modern digital technologies in the field of legal relations and in criminal proceedings. The transition to the priority of using digital sources has its own advantages and disadvantages. The presence of shortcomings is due to the imperfection of technical equipment, not always effective, high-quality and stable operation of the Internet, inconvenience and lack of necessary skills in the use of information resources by the elderly. The advantages, first of all, include ease of use, reduction of time, as well as free access when receiving public services by citizens.

Keywords: Digital technologies, Government, Internet resources, Digitalization, Internet fraud, Program, Investigation, Criminal process

Современное общество и государство невозможно представить без использования в повседневной жизни современных цифровых технологий. Данная тенденция охватила практически все сферы жизнедеятельности.

Если рассматривать такие области, как здравоохранение, деятельность правоохранительных органов, оказание государственных услуг, сферу образования и т. д., то можно найти большое количество цифровых источников и технологий, посредством которых и осуществляется деятельность всех этих и других сфер общества и государства [1].

Внедрение современных цифровых технологий охватило также и деятельность таких правоохранительных органов, как прокуратура, суд, органы полиции и т. д. Но каково назначение данных цифровых процессов? Какие они имеют преимущества и недостатки? В чем заключается их смысл? На эти и другие вопросы давайте постараемся найти ответы. Во-первых, переход к процессу цифровизации является постепенным процессом, требующим ответственного подхода к развитию данного процесса.

Первый этап перехода к цифровизации в Республике Казахстан ощутили сфера образования и здравоохранения.

Наиболее активно развивается процесс цифровизации в области юриспруденции. В первую очередь, если рассматривать деятельность правоохранительных органов, то можно выделить существенные изменения в делопроизводстве органов полиции, прокуратуры и судов, которые массово стали переходить на электронный формат работы. Так, например, внедрение системы ЕРДР, различных баз данных, которые содержат в себе информацию о преступниках, о фактах совершенных правонарушений, о наличии судимости, о нахождения лиц на различных учетах, о дактилоскопических учетах не только упрощают работу правоохранительных органов, но и дисциплинируют всех участников уголовного процесса. Также широкий спектр цифровых технологий в сфере правоохранительной деятельности предает гласности и прозрачности всем процессам в ходе производства процессуальных действий. Эффективность работы таких общедоступных информационных систем, как судебный кабинет, электронное правительство и ЕНИС доказана признанием и удобством использования гражданами.

Однако, как и любые нововведения, современные цифровые системы имеют ряд своих как преимуществ, так и недостатков. Так, например, можно выделить следующие недостатки современных цифровых технологий в области юриспруденции:

– отсутствие совершенства технических возможностей цифровых информационных процессов;

– отсутствие возможности использования цифровых возможностей людей более пожилого возраста;

– не всегда стабильная работа Интернет-ресурсов.

К преимуществам можно отнести: ускорение процессов правовых отношений, удобство в применении, возможность быстрого получения государственных услуг.

В современное время наблюдается рост тенденции перехода деятельности органов уголовного преследования к цифровому формату. Данный процесс отличается высокой степенью поэтапности, так как изначально было запланировано, например, в органах полиции, внедрить электронную регистрацию всех уголовных правонарушений, сообщений о фактах таковых деяний и т. д. Внедрение ЕРДР (Единый реестр досудебных расследований), который явился первым шагом к переходу на цифровой уровень досудебного расследования, несомненно, внесло свой вклад в упрощение процедуры регистрации уголовных правонарушений и, соответственно, это привело к ускорению данного процесса [2].

Теперь можно сказать, что процесс регистрации уголовных правонарушений может регулироваться принципом «прозрачности и открытости», как для будущих участников уголовного процесса, так и для надзорных органов, соответственно, и факты сокрытия правонарушений должны свестись к нулю. Но так ли это на самом деле? Как уже упоминалось выше, процесс перехода к цифровизации правоохранительных органов характеризуется поэтапным и постепенным переходом. Соответственно, первым этапом является переход к регистрации правонарушений, сообщений о фактах уголовных деяний, рапортов должностных лиц в едином реестре. Данное нововведение получило свое закрепление на законодательном уровне, так как теперь положения уголовно-процессуального кодекса Республики Казахстан гласят, что все проявления фактов уголовных правонарушений должны

быть зарегистрированы в ЕРДР в течение суток. В соответствии с этим, прокуратура должна осуществлять высший надзор за исполнением данного положения УПК РК.

Для того чтобы в полной мере перейти к «безбумажному», электронному делопроизводству в правоохранительных органах, примерно к 2018 г. начинает нарастать тенденция к расследованию уголовных дел в цифровом формате. Однако и данное мероприятие было решено проводить постепенно, начиная расследовать в электронном формате на первоначальном этапе преступления небольшой тяжести, оставив расследование тяжких, особо тяжких, многоэпизодных преступлений, многотомных уголовных дел на более поздний срок, нежели чем расследование преступлений небольшой и средней тяжести [3. С. 244].

На сегодняшний день переход к электронному уголовному делу охватил практически все подразделения следствия и дознания в органах полиции Казахстана. По нашему мнению, опыт перехода к регистрации уголовных правонарушений в едином реестре носит позитивный характер, так как он не только ускоряет и упрощает процесс регистрации правонарушения, но и дисциплинирует участников уголовного процесса, в том числе органы уголовного преследования: следствия и дознания. Постепенный и плавный процесс перехода к электронному формату уголовного процесса выражается в следующих этапах: разработка и внедрение информационной системы ЕРДР; внедрение ИС «Торелик», которая позволяет автоматизировать судебную систему; создание модуля «Электронное уголовное дело» на базе ИС ЕРДР, что позволяет автоматизировать стадии досудебного расследования и прокурорского надзора [4. С. 66].

Электронное уголовное дело имеет ряд следующих преимуществ:

– Значительная экономия времени производства процессуальных действий.

– Сокращение сроков расследования и получения санкций.

– Отражение принципа «прозрачности, открытости и доступности».

– Минимизация рисков фальсификации и сокрытия фактов совершенных уголовных правонарушений [5. С. 422].

– Возможность иметь доступ к материалам уголовного дела в любое время в формате онлайн.

– Исключение утери уголовных дел.

– Возможность ведения постоянного контроля и надзора за осуществляемыми органом уголовного преследования процессуальных действий и т. д. [6. С. 320].

В заключение хотелось бы отметить, что, по нашему мнению, опыт цифровизации уголовного процесса и деятельности органов уголовного преследования имеет позитивную сторону, однако не всегда стабильная работа интернет-ресурсов, несовершенство качества работы электронных инструментов, посредством которых осуществляется уголовное производство, а также недостаточные знания сотрудников правоохранительных органов в области работы с электронными источниками уголовного преследования могут лишь, наоборот усугубить и осложнить процесс, как досудебного расследования, так и на стадии судебного процесса. По нашему мнению, качественное обучение сотрудников правоохранительных органов навыкам использования электронных источников в уголовном процессе, а также совершенствование и улучшение состояния модуля «Электронное уголовное дело» смогли бы улучшить качество производства процессуальных действий и принятия решений в рамках конкретных уголовных дел.

Список литературы

1. Конституция РК, принятая на республиканском референдуме 30 августа 1995 года.
2. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК.
3. Манова Н. С., Францифоров Ю. В. Уголовный процесс: учебное пособие. Москва: Юрайт, 2020. 244 с.
4. Скурко Е. В. Состязательный процесс. Москва: Юридический центр, 2018. 66 с.
5. Францифоров Ю. В., Манова Н. С. Уголовный процесс. Учебник и практикум. Москва: Юрайт, 2020. 422 с.
6. Шаталов А. С., Крымов А. А. Уголовный процесс. Практикум. Москва: Проспект, 2020. 320 с.

Э. Ю. Латыпова,
кандидат юридических наук, доцент,
заведующий кафедрой уголовного права и процесса,
Казанский инновационный университет имени В. Г. Тимирясова

О ЦИФРОВИЗАЦИИ КАК СРЕДСТВЕ ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ В НЕКОТОРЫХ НАПРАВЛЕНИЯХ МЕДИЦИНСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Одним из перспективнейших направлений современной правовой действительности является повсеместное внедрение цифровых средств и информационно-коммуникационных технологий в существующие общественные отношения. Автор рассматривает возможности внедрения цифровых технологий в отдельные виды медицинской деятельности, выделяются причины и условия коррупционного поведения участников медицинской деятельности. Анализируется цифровизация сферы здравоохранения и использование медицинских информационных систем и технологий как одно из действенных средств противодействия коррупции.

Ключевые слова: противодействие коррупции, цифровизация, медицинская деятельность, врачебная тайна, квотирование, медицинские информационные системы и технологии

ABOUT DIGITALIZATION AS A MEANS OF COUNTERING CORRUPTION IN SOME AREAS OF MEDICAL ACTIVITY

Abstract. One of the most promising areas of modern legal reality is the widespread introduction of digital tools and information and communication technologies into existing public relations. The author examines the possibilities of introducing digital technologies into certain types of medical activities, highlights the causes and conditions of corrupt behavior of participants in medical activities. The article analyzes the digitalization of the healthcare sector and the use of medical information systems and technologies as one of the effective means of combating corruption.

Keywords: Anti-corruption, Digitalization, Medical activity, Medical secrecy? Quotas, Medical information systems and technologies

Введение. Активное внедрение в сферу здравоохранения информационно-коммуникационных технологий является существенным вектором улучшения эффективности государственного управления в данной сфере. Здоровье является одним из важнейших благ человека, гарантируемых Конституцией Российской Федерации, соответственно, улучшение его является значимой задачей государства. Однако повышение качества и оперативности предоставления медицинских услуг, к сожалению, является одним из возможных факторов коррупции и повышения коррупционных рисков. Применительно к сфере здравоохранения определенную сложность представляет также разграничение взятки как коррупционного преступления и благодарности, так как, по данным А. В. Мещеряковой и А. П. Мазуренко, «подарки и деньги работникам медицины граждане давали в 52 % случаев» [5. С. 181]. В то же время коррупция в сфере здравоохранения влечет возможное ухудшение здоровья, угрозу для жизни или причинение человеку страданий.

Основная часть. Счетная пала выявила ряд системных проблем, ухудшающих качество и доступность медицинской помощи населению, а именно: а) несовершенство нормативно-правового регулирования при формировании региональных перечней лекарственных препаратов, отпускаемых бесплатно или с 50 %-й скидкой; б) недостаточность нормативно-правового определения источников финансового обеспечения оказания высокотехнологичной помощи детям; в) отсутствуют или не утверждены стандарты оказания медицинской помощи по ряду распространенных заболеваний, по которым лечение оказывается бесплатно и др. [5. С. 181]. В частности, региональные власти должны обеспечивать больных редкими (орфанными) заболеваниями лекарственными препаратами в полном объеме и бесплатно. Однако, зачастую такое финансирование предусматривается не в полном объеме, и нуждающийся в таком лечении либо вынужден отказываться от него (что в ряде случаев приводит к существенному ухудшению его здоровья или даже смерти), либо приобретает дорогостоящие препараты за собственные средства, либо может использовать коррупционные варианты решения возникшей проблемы.

Коррупционные правонарушения в медицинской деятельности могут быть установлены при проведении различного рода грантовой деятельности при распределении бюджетных средств, при этом проведение торгов в электронной форме во многом предотвращает разного рода злоупотребления, делая такую деятельность более прозрачной.

Можно наблюдать достаточно хорошее финансирование медицинских организаций в крупных городах России (так называемых «миллионниках»), что позволяет закупать новейшее дорогостоящее оборудование; выделяются квоты на высокотехнологичную помощь и др. Однако на периферии финансирование более скудное и вызывает постоянные нарекания. Как правильно отмечают А. В. Мещерякова и А. П. Мазуренко, ряд вопросов можно разрешить с помощью грамотного распределения государственного задания (муниципального задания, квот) между государственными и частными клиниками, а также путем формирования тарифов,

отражающих реальную стоимость услуг [5. С. 182]. Но зачастую основные объемы квот выделяются государственным медицинским учреждениям, а частные клиники получают гораздо меньше средств, что минимально покрывает их потенциальные возможности.

К сожалению, определенные коррупционные риски могут присутствовать в медицинской деятельности при квотировании отдельных видов медицинской деятельности. Обычный порядок получения медицинской помощи по квоте заключается в следующем: 1. Обращение к лечащему врачу в поликлинике (обычно по месту жительства), или напрямую в специализированный медицинский центр. 2. При подозрении на серьезное заболевание лечащий врач обязан выдать направление для обследования в специализированной медицинской организации. 3. Специалисты специализированной медицинской организации комиссионно принимают решение о направлении на необходимое лечение в рамках выделенного количества квот. Нужно учитывать, что ведение документации в электронном виде в значительной степени ускоряет оказание медицинской помощи, в том числе высокотехнологичной [6. С. 152], тем самым снижая количество коррупционных рисков.

Соответственно, на любом из этих этапах возможны коррупционные правонарушения и злоупотребления. Так, зачастую лечащий врач широкой практики не обладает должным опытом в выявлении сложных и (или) редких заболеваний, либо у него не хватает выделенного регламентом времени для проведения осмотра в должном объеме. За назначением и (или) получением любого анализа надо снова обращаться к терапевту, что усложняет и удлиняет сам процесс диспансеризации или подготовки к госпитализации. Поэтому часть пациентов обращается в коммерческие центры за платной медицинской помощью, а некоторая часть «договаривается» о более быстром обслуживании за незаконное вознаграждение. Традиционно медицинская деятельность считается одной из самых коррумпированных [2. С. 53], хотя, отметим ради справедливости, в настоящее время таких фактов выявляется все меньше [4. С. 58]. Однако повторимся – в ряде случаев граждане вынужденно участвуют в коррупционных действиях, желая быстрее получить необходимую медицинскую помощь (например, квоты на лечение и операции, рецепты на медицинские препараты, возможность пройти медицинское обследование на необходимом аппарате или оборудовании без предварительной записи и многомесячного ожидания). В частности, даже бесплатное обследование на аппарате УЗИ зачастую возможно не ранее, чем через две-три недели, тогда как для больного счет иногда идет на часы.

Постоянно на слуху проблемы при оказании высокотехнологичной помощи онкологическим больным. Регулярно поднимаются вопросы о возможности оказания такой дорогостоящей помощи в частных онкологических центрах бесплатно. И с помощью государственно-частного партнерства это становится реальным [6. С. 30]. Так, при наличии медицинских показаний можно получить бесплатное лечение за счет средств, выделенных бюджетом субъекта Российской Федерации. Однако сама возможность получения бесплатно дорогостоящего лечения уже создает благоприятные условия для злоупотреблений, в том числе коррупционного характера. Особенно актуально предупреждение таких коррупционных злоупотреблений при

обращении за медицинской помощью инвалидов [1. С. 66–70]. Сложность контроля за справедливым распределением квот также осложняется и тем фактом, что зачастую за высокотехнологичной помощью обращаются иногородние (по некоторым видам операций таких лиц может быть более 75 % [8. С. 145]), что также оставляет значительный простор для коррупционных рисков.

Можно полагать, что при предоставлении реабилитационных услуг также возможны коррупционные проявления, когда за «вознаграждение» предлагается продвижение по очереди. При этом стоимость реабилитации при отдельных заболеваниях очень высока, и вопросы о ее рентабельности практически не поднимаются [9. С. 47].

Коррупционные злоупотребления в достаточно большом количестве наблюдались в 2020–2021 гг. при проведении вакцинации, в том числе против новой коронавирусной инфекции SARS-CoV-2, когда за незаконное вознаграждение врачи (медсестры) проставляли отметку о вакцинации, реально не проводя саму процедуру вакцинации, о чем мы уже писали ранее [3. С. 366–371].

Полагаем, что одним из действенных средств антикоррупционной политики в медицине может стать повсеместная цифровизация, широкое использование медицинских информационных систем и технологий, которая начинается буквально с момента регистрации пациента на прием по телефону либо через интернет-портал к конкретному специалисту (частично данная опция уже внедрена через систему сайта Госуслуг). Постепенно вводятся электронные медицинские карты пациента, в ряде регионов проходят успешные эксперименты по внедрению специальных браслетов с электронной базой данных о состоянии здоровья пациента и специальной тревожной кнопкой, которая может информировать об ухудшении состояния пациента [7]. При этом в ряде медицинских учреждений уже используются браслеты для идентификации пациентов [10]. Однако широкое применение указанных технологий также невозможно вследствие недостатка государственного финансирования, что, в свою очередь, также может иметь определенные коррупционные риски. Расширение же цифровизации в здравоохранении может способствовать улучшению удовлетворенности населения оказываемой ему медицинской помощью, ее оптимизации и снижению различного рода затрат, связанных, среди прочего, с дублированием некоторых инициатив на региональном уровне.

Отдельный интерес может быть связан с особенностями сохранения врачебной тайны, так как в настоящее время активно внедряется внедрение медицинских карточек и документов в электронной форме, что, в свою очередь, может представлять определенную опасность в отношении защиты персональных данных пациента, создавая опасность не только коррупционных правонарушений, но и различного рода мошеннических действий в отношении отдельных пациентов.

Выводы и предложения. Нам представляется, что введение цифровых технологий в медицинскую деятельность может в значительной степени способствовать снижению количества коррупционных рисков. В данной работе мы показали лишь несколько направлений возможных коррупционных злоупотреблений, полагаем, что их может быть намного больше. Соответственно, требуется дальнейшее, более глубокое исследование противодействия коррупции в медицинской деятельности, чему, несомненно, будет способствовать использование цифровых технологий.

Полагаем, что именно цифровизация в сфере здравоохранения будет, с одной стороны, способствовать наиболее эффективному удовлетворению потребностей населения в качественной медицинской помощи, и, с другой стороны, наиболее адекватно противодействовать коррупции в исследуемой сфере, исключая возможность фальсификации медицинских документов.

Список литературы

1. Гильманов Э. М., Урмаева Е. Н. Прокурорский надзор за соблюдением прав инвалидов // Время науки: сборник научных трудов II Международной научно-практической конференции. Ставрополь, 2020. С. 66–70.

2. Гильфанова А. Ш., Латыпова Э. Ю. Некоторые аспекты коррупции в сфере здравоохранения // Диалектика противодействия коррупции: материалы IV Всероссийской научно-практической конференции. Институт экономики, управления и права (г. Казань). Казань: Познание, 2014. С. 106–107.

3. Латыпова Э. Ю., Мусина Р. Р., Гильманов Э. М. Уголовная ответственность за преступления, связанные с вакцинацией, и противодействие им со стороны прокуратуры // Прокуратура Российской Федерации: вектор развития и роль в формировании демократического правового государства: сборник материалов Междунар. науч.-практ. конф. Чебоксары, 29–30 октября 2021 г.: в 2 ч. Чебоксары: Изд-во Чуваш. ун-та, 2021. Ч. 1. С. 366–371.

4. Латыпова Э. Ю. О коррупционном поведении врачей // Вопросы реализации государственной политики в области противодействия коррупции: сборник материалов. Университет прокуратуры Российской Федерации. Казанский юридический институт (филиал). Казань, 2020. С. 58–62.

5. Мещерякова А. В., Мазуренко А. П. Цифровизация как средство антикоррупционной правовой политики в сфере здравоохранения // Вестник Костромского государственного университета. 2019. Т. 25, № 3. С. 181–184.

6. Новый опыт в здравоохранении: могут ли воронежцы рассчитывать на бесплатную медицинскую помощь в частном онкоцентре? // Главный врач Юга России. 2014. № 1 (38). С. 30–31.

7. Пациентам могут начать выдавать браслеты с доступом к истории болезни // Медицинское обозрение. URL: https://regions.ru/news/2602951/ (дата обращения: 01.09.2022).

8. Терещенко А. В., Трифаненкова И. Г., Алхимова Д. В., Юдина Н. Н. Оказание высокотехнологичной помощи пациентам с витреоретинальной патологией: опыт организации и перспективы // Медицина. 2017. № 3. С. 145–155.

9. Шурыгин Г. И. Реабилитация государственная и общественная: из опыта областной психиатрической больницы № 8 // Психиатрия. 2012. № 4 (56). С. 47–51.

10. URL: https://rosbraslet.ru/news/meditsinskie-braslety-dlya-patsientov-i-vrachej/ (дата обращения: 01.09.2022).

Э. Ю. Латыпова,
кандидат юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова
Р. Р. Мусина,
заместитель декана юридического факультета
по научной и воспитательной работе,
Казанский инновационный университет имени В. Г. Тимирясова
Э. М. Гильманов,
старший преподаватель кафедры уголовного права и процесса,
Казанский инновационный университет имени В. Г. Тимирясова

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАССЛЕДОВАНИИ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ

Аннотация. В настоящее время одним из самых инновационных направлений в расследовании преступлений является использование различного рода цифровых технологий. Существенное место среди всех преступлений занимают преступления против собственности, часть из которых может совершаться с использованием цифровых технологий. В то же время и при расследовании экономических преступлений также активно применяются цифровые технологии. В представленном материале анализируются особенности расследования некоторых экономических преступлений с учетом использования отдельных цифровых технологий. Полагаем, что перспективы использования цифровых технологий в криминалистике при расследовании отдельных видов преступлений являются поистине прорывными!

Ключевые слова: экономические преступления, цифровизация, цифровые технологии, расследование преступлений

DIGITAL TECHNOLOGIES IN THE INVESTIGATION OF ECONOMIC CRIMES

Abstract. Currently, one of the most innovative areas in the investigation of crimes is the use of various kinds of digital technologies. A significant place among all crimes is occupied by crimes against property, some of which can be committed using digital technologies. At the same time, digital technologies are also actively used in the investigation of economic crimes. The presented material analyzes the features of the investigation of some economic crimes, taking into account the use of certain digital technologies. We believe that the prospects for the use of digital technologies in criminology in the investigation of certain types of crimes are truly breakthrough!

Keywords: Economic crimes, Digitalization, Digital technologies, Crime investigation

Введение. Генеральная прокуратура Российской Федерации ежегодно фиксирует рост преступлений, совершаемых с использованием цифровых технологий. Соответственно, необходимо использовать указанные технологии и при расследовании совершенных с их применением преступлений.

Актуальность темы напрямую вытекает из приоритетов распространения и использования информационных технологий в социально-экономической среде.

Среди цифровых технологий, применяемых при расследовании экономических преступлений, одним из первых является использование современных цифровых камер. Однако спектр их применения может быть более широким [3. С. 264], чем просто фиксация какого-либо изображения.

Динамика использования цифровых технологий при расследовании преступлений, в том числе экономической направленности, повышается с возникновением новых информационно-телекоммуникационных технологий, а также с появлением и внедрением новейшего высокотехнологичного оборудования и возможностями использования искусственного интеллекта [1].

Основная часть. Мошенничество с помощью методов социальной инженерии практически не оставляет клиентам банков (особенно их виртуальных представительств) шансов вернуть деньги обратно, на свой банковский счет. Такая ситуация возникает в случае, если лицо под влиянием обмана само совершает определенную банковскую операцию, либо самостоятельно разглашает данные, позволяющие ее провести [8. С. 108]. В таком случае банковская карта будет считаться скомпрометированной, что приводит к ситуации, когда кредитные организации не будут нести никакой ответственности за пропажу с нее денежных средств. Заметим, что пункт с подобным содержанием считается стандартным для обычных банковских договоров. Соответственно, раскрыть такое преступление также чрезвычайно сложно, хотя количество потерпевших от таких мошенничеств постоянно растет.

Необходимо учитывать, что каждый государственный орган в настоящее время должен вести в электронной форме соответствующие реестры, по которым заинтересованные лица могут получить необходимую информацию (например, можно проверить выданную доверенность и условия ее действия на сайте Федеральной нотариальной палаты и т. п.).

В последнее время в судебной и следственной практике достаточно часто встречаются случаи так называемого виртуального вымогательства, которое становится массовым явлением с большим количеством потерпевших, однако данный вид вымогательства имеет значительную латентность, так как жертвы опасаются обращаться в полицию из-за боязни огласки компрометирующей информации [6. С. 38] и общественного порицания своего поведения.

Так, на брифинге, посвященном работе Главного следственного управления МВД по РТ, первый заместитель начальника ГУ МВД по РТ М. Фролова сообщила, что 30-летняя преподавательница вуза из Казани отдала 2,8 млн рублей брачному аферисту, заложив квартиру, так как он угрожал разместить ее интимные фотографии на сайте вуза, чтобы они не попали в сеть Интернет [5]. К сожалению, сам факт задержания вымогателя, использующего виртуальный шантаж, вовсе не гарантирует привлечение данного лица к уголовной ответственности, так как в подавляющем большинстве случаев либо уголовное дело не возбуждается, либо ранее возбужденное дело прекращается по разным основаниям и передается в архив. Считаем необходимым в этой связи усилить контроль со стороны органов прокуратуры как за оперативно-розыскной деятельностью, так и за производством дознания и предварительного расследования в части оснований для прекращения уголовного дела по разным основаниям [6. С. 113].

Одним из достаточно традиционных в последнее время является использование при расследовании преступлений цифровых фотокамер, которые позволяют фиксировать изображение с достаточно большим разрешением, что в дальнейшем можно использовать при увеличении данного изображения. Оптимальный режим фотосъемки, по верному замечанию А. С. Волкова, позволяет получить фотоизображения следов рук с достаточной резкостью для назначения идентификационной дактилоскопической экспертизы по фотоизображению следов рук, полученных, например, с денежной купюры посредством использования паров йода, который в дальнейшем испаряется, делая затруднительным дальнейшее использование данных следов [3. С. 124]. Аналогичные действия можно произвести и на других финансовых документах, получая необходимую доказательную базу.

Использование при совершении преступлений поддельных документов также во многом объясняется высоким качеством таких подделок вследствие использования современной копировально-множительной техники, что весьма осложняет раскрытие и расследование преступлений, так как зачастую индивидуальные идентификационные признаки отсутствуют или являются очень незначительными.

По мнению О. А. Соколовой, весьма перспективным направлением установления давности следов пальцев рук является метод лазерной флюорографии (флюоресценции), основанный на различии в цвете люминисценции следов в зависимости от времени их оставления [10. С. 96]. Такие следы можно фотографировать методом цветоделительной съемки с использованием различных светофильтров; более того, потожировое вещество следа не разрушается, и его можно использовать для других методов исследования.

Как отмечается Н. Р. Шевко, «Татарстанская прокуратура в 2016 г. практически стала главным органом по надзору за исполнением провайдерами всей России судебных решений по блокировке запрещенных сайтов. Президент РФ Владимир Путин подписал поручения о разработке в стране системы мониторинга информационных угроз. Тем временем аналог таковой уже был разработан в Татарстане – эту работу проводила прокуратура РТ, выявляя и блокируя доступ пользователям к материалам пяти категорий, включая экстремизм и терроризм» [12. С. 104].

Система контроля противозаконных материалов ICM появилась в Татарстане в 2016 г. С ее помощью было выявлено более 18 тыс. сайтов, содержавших ссылки и цитаты на материалы из реестра экстремистских материалов Минюста РФ и признаки нарушения федерального законодательства. Проверкой этого контента занимались 17 прокуроров (сотрудники центрального аппарата прокуратуры РТ, а также прокуратур Казани, Апастово, Нижнекамска и Челнов), по решению которых одним нажатием кнопки были направлены на блокировку данные о 1 670 сайтах для потребителей наркотиков, 1 153 онлайн-казино, 945 сайтах по пропаганде суицида и 577 сайтах с детской порнографией [12. С. 104].

Используя сервер ICM, можно проводить оперативно-розыскные мероприятия, блокировать деньги на счетах или номера телефонов, и даже задерживать преступников. Соответственно, возможна борьба не только с распространением определенной информации, но и нанесение «удара» по самой инфраструктуре.

Таким образом, к цифровым технологиям расследования преступлений, помимо вышеперечисленных, можно отнести технологии восстановления и обнаружения

данных, собирание доказательств, криминалистический анализ цифровых средств и данных, необходимых для раскрытия и расследования преступлений [11, с. 164], включая сбор, хранение, анализ и представление данных, полученных любыми устройствами, фиксирующими информацию в цифровой сфере, вплоть до использования при расследовании преступлений искусственного интеллекта [2. С. 65].

Заключение. Практически единственным действенным способом предотвращения совершения экономических преступлений видится повышение информированности населения об опасности передачи различного рода информации (особенно коммерческого характера) посторонним лицам и возможности использования такой информации в противоправных целях. В среде несовершеннолетних возможно проведение лекций о безопасном поведении в сети Интернет, с целью повышения их информированности о нежелательности подобных действий.

Эффективным способом противодействия подделке документов может являться повсеместное введение электронного документооборота, так как обычные бумажные документы легко подделать с помощью современных копировально-множительных аппаратов.

Глобализация информационных телекоммуникационных процессов приводит к выходу экономических преступлений за границы территории России, закрепляя их международный и даже транснациональный характер, не ограничивая территорией отдельного государства и повышая их общественно опасный характер.

Список литературы

1. Бегишев И. Р., Латыпова Э. Ю., Кирпичников Д. В. Искусственный интеллект как правовая категория: доктринальный подход к разработке дефиниции // Актуальные проблемы экономики и права. 2020. Т. 14, № 1. С. 79–91.

2. Белова М. А. Использование искусственного интеллекта в расследовании преступлений / В сборнике: Цифровые трансформации в развитии экономики и общества. Материалы XVIII Международной научно-практической конференции. В 4-х томах. Воронеж, 2021. С. 65–69.

3. Волков А. С. Применение цифровых технологий в ходе расследования преступлений в экономической сфере // Экономическая безопасность и качество. – 2018. № 2 (31). С. 124–126.

4. Гильманов Э. М., Кирпичников Д. В. О необходимости разработки методики расследования преступлений в сфере обращения цифровой информации // Актуальные проблемы государства и права. 2020. Т. 4, № 14. С. 262–277.

5. Кривопатре Е. На уловки 32-летнего многократно судимого за разбои и грабежи жителя Казани попались три жительницы Татарстана // https://www.tatar-inform.ru/news/2019/04/03/647114/ (дата обращения: 01.09.2022).

6. Латыпова Э. Ю. Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Oeconomia et Jus. – 2019. – № 2. – С. 35–45.

7. Латыпова Э. Ю., Ключникова К. Е. Проблемы уголовной ответственности за вымогательство с использованием виртуального шантажа / Информационные технологии в деятельности органов прокуратуры. Сборник материалов II Всероссийской научно-практической конференции. Казань, 2019. С. 110–113.

8. Латыпова Э. Ю., Мусина Р. Р. Некоторые проблемы мошенничеств с помощью использования банковской карты с голосовым помощником / Информационные технологии в деятельности органов прокуратуры. Сборник материалов II Всероссийской научно-практической конференции. Казань, 2019. С. 107–109.

9. Мусина Р. Р. К вопросу о развитии уголовной ответственности за преступления против собственности в законодательстве России // Oeconomia et Jus. 2019. № 1. С. 64–72.

10. Соколова О. А. Использование результатов диагностических экспертиз по следам человека в уголовном судопроизводстве // Вестник Московского университета МВД России. 2019. № 1. С. 94–98.

11. Соловьева С. М. Применение цифровых технологий в криминалистике // Молодой ученый. 2019. № 51 (289) С. 161–164.

12. Шевко Н. Р. Информационные технологии в деятельности прокуратуры: преимущества и недостатки / В сборнике: Информационные технологии в деятельности органов прокуратуры. Сборник материалов II Всероссийской научно-практической конференции. Казань, 2019. С. 102–106.

О. И. Лепешкина,
кандидат юридических наук, доцент,
Северо-Западный институт управления – филиал Российской академии
народного хозяйства и государственной службы
при Президенте Российской Федерации

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РОССИИ

Аннотация. Целью исследования является определение основных направлений реализации государственной политики в области противодействия киберпреступности, а также обозначение перспективы развития ее нормативного правового регулирования. В настоящее время нет единого международного правового механизма противодействия киберпреступности, имеющей транснациональный характер, что затрудняет сотрудничество государств в данной области, развитие и унификацию национального законодательства. Автором сделан вывод о необходимости принятия Стратегии кибербезопасности, Закона «О противодействии киберпреступности» и соответствующей государственной программы.

Ключевые слова: цифровые технологии, киберпреступность, киберпреступление, противодействие киберпреступности, высокотехнологичная преступность, компьютерные преступления, кибербезопасность, киберпространство

THE PRINCIPAL DIRECTIONS OF ANTI-CYBERCRIME IN RUSSIA

Abstract. The goal of this article is to define the principal directions of anti-cybercrime in realization of anti-cybercrime state politics, and also to mark perspectives it's law regulation. There is not the international law mechanism of anti-cybercrime in this time. Therefore, there is difficulty of international collaborate with states about anti-

cybercrime and also development and unification national laws. Author makes conclusion about necessity adoption of Strategy on cybersecurity, the Law “About anti-cybercrime” and state program on this sphere.

Keywords: Digital technology, Cybercrime, Anti-cybercrime, High-tech crime, Computer crime, Cybersecurity, Cyberspace

Введение. Киберпреступность в настоящее время уже представляет угрозу национальной безопасности, что признает все мировое сообщество. Основная часть преступлений с использованием информационных технологий корыстные, совершаемые в кредитно-финансовой сфере, и которые наносят государству значительный экономический ущерб, способный спровоцировать финансовый кризис. Кибератаки осуществляются на критическую информационную инфраструктуру, под угрозой и международная информационная безопасность.

Кроме того, преступления в сфере цифровых технологий имеют транснациональный характер и могут затрагивать интересы нескольких государств.

Вместе с тем пока нет единого международного правового механизма противодействия данным преступлениям, что осложняет взаимодействие государств в этой области, как и затрудняет развитие и унификацию национального законодательства государств.

Наличие такого правового механизма необходимо для решения вопросов выдачи лиц, совершивших киберпреступления, оказания взаимной правовой помощи и иного правоохранительного содействия, ареста и конфискации преступных доходов.

С целью противодействия высокотехнологичной преступности Российская Федерация 30 июля 2021 г. внесла в Генеральную Ассамблею ООН проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (резолюция Генеральной Ассамблеи ООН 75/980, принятая на 75-й сессии 10 августа 2021 г.) [8].

На региональном уровне с целью противодействия киберпреступности 23 ноября 2001 г. Советом Европы была принята Конвенция о преступности в сфере компьютерной информации (Конвенция о киберпреступности) [2]. Данную Конвенцию ратифицировали 66 государств, в том числе из не членов Совета Европы Израиль, США и Япония. Российская Федерация сочла положения пункта «b» ст. 32, согласно которому доступ к компьютерным данным другого государства может осуществляться и без его согласия, вмешательством в юрисдикцию и отказалась подписывать Конвенцию.

Кроме того, 17 ноября 2021 г. Комитет министров Совета Европы принял Второй дополнительный протокол к Конвенции о киберпреступности о расширении сотрудничества и раскрытии электронных доказательств. Данный протокол был открыт для подписания государствами-участниками Конвенции 12 мая 2022 г.

Таким образом, в настоящее время для эффективного противодействия киберпреступности и другим преступлениям, совершаемым с использованием информационных технологий, требуется расширение сотрудничества государств в данной области и сближение их правовых систем.

Основная часть. Стратегия национальной безопасности Российской Федерации в качестве угрозы информационной безопасности указывает на распространенность

преступлений, совершаемых с использованием информационно-коммуникационных технологий, и стратегическим национальным приоритетом является их предупреждение, выявление и пресечение (п. 42) [3].

Центральный банк Российской Федерации ежегодно публикует данные об атаках на информационную инфраструктуру клиентов – физических и юридических лиц. Так, в 2021 г. общее количество и объем операций, совершенных без согласия клиентов, увеличились на 33,8 и 38,8 % соответственно. Объем таких операций составил 13 582,23 млн руб. (в 2020 г. – 9777,3 млн руб.), количество операций 1 035,01 тыс. ед. [5]

Данные статистики ГИАЦ МВД России показывают постоянный рост в последние годы преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации: в 2019 г. было зарегистрировано 294 409 (рост на 68,5 %) преступлений, в 2020 г. – 510 396 (рост на 73,4 %), в 2021 г. – 517 722 (рост на 1,4 %) [7].

Киберпреступность, являющаяся криминологической категорией, может быть определена как совокупность киберпреступлений.

Киберпреступление – это преступление, полностью совершенное в киберпространстве.

Такое определение понятия киберпреступления соответствует указанному в Международном стандарте Международной организации по стандартизации «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности» (ISO/IEC 27032:2012 Information Technology – Security Techniques – Guidelines for Cybersecurity) [9]. В соответствии с положениями этого Международного стандарта ИСО киберпреступление – это «преступная деятельность, при которой сервисы или приложения киберпространства являются орудием или целью преступления или при которой само киберпространство является источником, инструментом, целью или местом преступления».

Поэтому следует согласиться с В. Ф. Джафарли в том, что киберпреступления в отличие от иных преступлений с использованием информационно-коммуникационных технологий – только те, «основные действия и последствия которых происходят исключительно в киберпространстве» [1. С. 61–62].

В Содружестве Независимых Государств в настоящее время разрабатывается проект модельного закона «О противодействии киберпреступности». Полагаем, что принятие такого закона в России настоятельно необходимо и позволит создать правовой механизм противодействия киберпреступности, скоординировать деятельность государственных органов, органов местного самоуправления, институтов гражданского общества, граждан и организаций по реализации государственной политики в данной области.

С учетом мирового опыта представляется целесообразным принять Стратегию кибербезопасности государства, в которой определить стратегические цели, задачи и основные направления государственной политики в области обеспечения кибербезопасности государства. Следует отметить, что Концепция Стратегии кибербезопасности Российской Федерации была размещена для обсуждения на официальном сайте Совета Федерации Федерального Собрания РФ еще в 2014 г.

Для последовательности реализации государственной политики в области противодействия киберпреступности может быть принята государственная программа по противодействию киберпреступности.

По мнению автора, к основным направлениям противодействия киберпреступности можно отнести следующие: 1) совершенствование организации деятельности правоохранительных и судебных органов, а также органов прокуратуры; 2) совершенствование системы подготовки, профессиональной переподготовки и повышения квалификации кадров правоохранительных и судебных органов, а также органов прокуратуры; 3) осуществление контроля доступа и обработки персональных данных; 4) обеспечение безопасности предоставления финансовых услуг в электронной форме; 5) повышение уровня киберграмотности клиентов финансовых организаций; 6) взаимодействие государственных органов с провайдерами хостинга, операторами связи, оказывающими услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», операторами поисковых систем, владельцами социальных сетей, регистраторами доменных имен и операторами подвижной радиотелефонной связи; 7) повышение степени информированности общества в области противодействия киберпреступности; 8) повышение эффективности профилактики киберпреступлений; 9) развитие государственно-частного взаимодействия; 10) мониторинг правоприменения; 11) развитие деятельности по лицензированию, сертификации и стандартизации в области технической защиты информации и обеспечения информационной безопасности; 12) развитие криптографической деятельности.

В числе мер по предупреждению киберпреступности важным является взаимодействие с институтами гражданского общества. В настоящее время активное сотрудничество правоохранительных и других контрольно-надзорных органов осуществляется с кибердружинами. Так, «Кибердружина» организации «Лига безопасного Интернета» представляет собой межрегиональное молодежное общественное движение, объединяющее волонтеров в России, государствах СНГ, Западной и Восточной Европе [6]. Целью кибердружин является выявление в сети Интернет противоправной информации.

Результаты деятельности кибердружин показывают их значительную роль в выявлении и расследовании киберпреступлений, что указывает на перспективность этого направления в профилактике киберпреступлений. Например, в субъекте Российской Федерации Белгородской области кибердружины были созданы еще в 2017 г. [4]

В 2019 г. депутатами «Единой России» был подготовлен законопроект «О кибердружинах».

Заключение. В заключение следует отметить, что для эффективного противодействия киберпреступности в России требуется соответствующая нормативная правовая база. Поэтому в ближайшей перспективе необходимо принять Закон «О противодействии киберпреступности» и Стратегию кибербезопасности.

Список литературы

1. Джафарли В. Ф. Криминология кибербезопасности: в 5 т. Т. 2: Уголовно-правовое обеспечение криминологической кибербезопасности / под ред. С. Я. Лебедева. Москва: Проспект, 2021. 280 с.

2. Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. // СПС «Гарант». URL: https://base.garant.ru/4089723/ (дата обращения: 05.03.2022).

3. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. № 400 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 05.03.2022).

4. Об организации деятельности кибердружин Белгородской области: Постановление Правительства Белгородской области от 22 мая 2017 г. № 181-пп // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/3100201705240004?rangeSize=20 (дата обращения: 22.07.2022).

5. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году. URL: https://cbr.ru/analytics/ib/operations_survey_2021/#:~: text=B 2021 году доля объема,— 0%2C00120%25)1. (дата обращения: 22.07.2022).

6. Официальный сайт Лиги безопасного Интернета. URL: http://www.ligainternet.ru/ (дата обращения: 22.07.2022).

7. Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/ (дата обращения: 04.03.2022).

8. Письмо Временного поверенного в делах Постоянного представительства Российской Федерации при Организации Объединенных Наций от 30 июля 2021 года на имя Генерального секретаря. URL: https://undocs.org/ru/A/75/98 (дата обращения: 20.03.2022).

9. ISO/IEC 27032:2012 Information Technology – Security Techniques-Guidelines for Cybersecurity. URL: https://www.iso.org/standard/44375.html (дата обращения: 30.03.2022).

Н. Д. Лопатина,
заведующий лабораторией, преподаватель,
Курский государственный политехнический колледж
С. С. Лопатин,
преподаватель,
Курский монтажный техникум

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ BIG DATA В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация. Исследование посвящено изучению роли Единой информационной системы в сфере закупок для обеспечения эффективности государственного заказа с точки зрения обеспечения конкуренции и экономии бюджетных денежных средств. Рассматриваются электронные торговые площадки, и обосновывается необходимость сокращения их количества в целях преодоления административных барьеров для субъектов предпринимательской деятельности. Оцениваются важность и значимость электронных сервисов с точки зрения определения путей их дальнейшего совершенствования.

Ключевые слова: государственные закупки, Единая информационная система в сфере закупок, государственный заказ, электронные торговые площадки, конкуренция, экономия, информационные технологии

IMPROVING THE MECHANISM OF PROCUREMENT FOR PUBLIC NEEDS USING DIGITAL TECHNOLOGIES

Abstract. The research is devoted to the study of the role of a Unified information system in the field of procurement to ensure the effectiveness of public procurement from the point of view of ensuring competition and saving budget funds. Electronic trading platforms are considered, and the need to reduce their number in order to overcome administrative barriers for business entities is justified. The importance and significance of electronic services is assessed from the point of view of determining ways to further improve them.

Keywords: Public procurement, Unified information system in the field of procurement, State order, Electronic trading platforms, Competition, Economy, Information technology

Сектор государственных закупок в Российской Федерации имеет большой потенциал. Развитие цифровых технологий позволяет делать государственные закупки максимально прозрачными, доступными для всех участников торгов, а также привлекать к участию социально ориентированные некоммерческие организации, которым нужна особая поддержка в развитии.

Ранее государственные закупки размещались на официальном портале в сети Интернет и предусматривали не только электронную, но и бумажную процедуру. Со временем цифровые технологии вытеснили бумажный документооборот, и осуществление государственного заказа стало носить наиболее открытый характер.

Единая информационная система в сфере закупок (далее – ЕИС) представляет собой интернет-портал, на котором размещается информация обо всех государственных закупках, о результатах проведенных процедур, об исполнении договоров и контрактов [3. С. 14]. Она содержит всеобъемлющую информацию об учреждениях, являющихся заказчиками, о планируемых конкурентных и неконкурентных процедурах, о контрактах или договорах, заключенных учреждениями.

ЕИС была создана во исполнение положений Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и Федерального закона от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и подзаконных нормативных актов [1. С. 30].

На первоначальном этапе создания ЕИС как от заказчиков, так и от поставщиков (подрядчиков, исполнителей) было огромное количество жалоб на ее работу, и на протяжении многих лет разработчики совершенствовали информационную систему во благо обеих сторон. На сегодняшний день с точки зрения формационного обеспечения государственного заказа произошел большой скачек в развитии ЕИС: она оперативно работает, позволяет аккумулировать большой объем инфор-

мации, предоставляет корректные сведения и быстро интегрирует их в систему. Таким образом, на сегодняшний день ЕИС представляет собой оплот государственного заказа, без которого его существование не представляется возможным.

Информационные технологии на сегодняшний день – фундамент, на котором строятся многие государственные системы [2. С. 108]. Для государственных торгов ЕИС – ядро, которое задает тенденцию развития информационных технологий, а также законодательной базы, строящейся вокруг обеспечения государственных нужд. Благодаря существованию Единой информационной системы торги являются открытыми в равной степени для всех участников, информация раскрывается в открытом доступе, что позволяет любому физическому или юридическому лице ознакомиться с ней.

В интернет-поле действуют отобранные операторы электронных площадок. Они представляют собой сайты, которые обеспечивают взаимодействия поставщика (подрядчика, исполнителя) и заказчика. Электронных торговых площадок в рамках Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» всего девять, в рамках Федерального закона от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» действует большее количество площадок. Для заказчика они бесплатны, для поставщиков (подрядчиков, исполнителей) действуют тарифы и условия, в соответствии с которыми они должны действовать на них.

Ситуация осложняется тем, что каждая торговая площадка обязывает поставщика (подрядчика, исполнителя) следовать своему порядку, который незначительно различается [5. С. 427]. Кроме этого, поставщикам (подрядчикам, исполнителям) сложно получить регистрацию на каждой площадке, отследить большое количество закупочных процедур на разных площадках и соблюсти порядок внесения и возврата денежных средств в счет обеспечения или комиссии за пользование ей. При этом тенденция такова, что количество торговых площадок стремится к увеличению. С каждым годом получают аккредитацию новые торговые площадки.

Нельзя забывать о том, что основной целью осуществления государственных закупок является создание конкуренции и экономия государственного бюджета [4. С. 34]. Создание Единой информационной системы и электронных торговых площадок представляет собой средство достижения этой цели. Усложнение электронных процедур приведет к тому, что эти цели не будут достижимы, учитывая, что доля государственного заказа в структуре отечественного бизнеса увеличивается. Организации и предприятия различных форм собственности должны иметь возможность участвовать в процедурах и развивать своей дело. Не каждый субъект малого и среднего предпринимательства имеет ресурсы и возможности для преодоления многочисленных административных барьеров, которые перешли и в сеть Интернет. Речь идет о регистрации на торговых площадках, времени, которое необходимо для проверки документов на каждой, о внесении денежных средств за приобретение сертификатов для пользования ими, о комиссиях площадок.

На наш взгляд, следует сократить количество электронных торговых площадок в рамках Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе

в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и Федерального закона от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», так как это усложняет поле деятельности поставщика (подрядчика, исполнителя) и делает государственный заказ не таким доступным.

В ближайшей перспективе основными целями развития ЕИС в сфере государственного заказа видится анализ существующих электронных сервисов с точки зрения определения путей их дальнейшего совершенствования, а также разработка новых механизмов цифрового взаимодействия участников закупочного процесса. Кроме того, дальнейшее цифровое развитие ЕИС представляется вполне логичным с учетом реализации программ цифровизации российской экономики и информационного общества.

Список литературы

1. Богданова А. В. Актуальные проблемы осуществления внешнего государственного финансового контроля за состоянием и управлением государственным долгом субъекта Российской Федерации // Финансовое право. 2019. № 6. С. 30–34.

2. Грачева Е. Ю., Соколова Э. Д. Финансовое право: учебник для средних специальных учебных заведений. 3-е изд., испр. и доп. Москва: Столица, 2020. 319 с.

3. Клещенко Ю. Г., Савченко М. М. Финансовый контроль как один из факторов обеспечения финансовой безопасности // Финансовое право. 2019. № 5. С. 14–18.

4. Кузнецова М. В. Коррупция в сфере государственных (муниципальных) закупок // Вестник Уральского финансово-юридического института. 2016. № 1 (3). С. 34–39.

5. Паулов П. А., Понамаренко С. С. Актуальные проблемы государственного регулирования в сфере закупок // Современные научные исследования и разработки. 2019. № 8 (16). С. 427–428.

А. И. Ляхова,
кандидат юридических наук,
Белгородский государственный
национальный исследовательский университет

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: ПРОБЛЕМЫ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ

Аннотация. В статье рассматриваются вопросы нормативного регулирования использования информационных технологий в сфере уголовного судопроизводства на основе анализа действующих международных актов и национального законодательства. В ходе проведенного исследования сделан вывод о необходимости разработки и законодательного закрепления понятий «электронное правосудие», «электронное доказательство» в целях реализации прав и законных интересов участ-

ников уголовно- процессуальной деятельности, улучшения доступа к правосудию и модернизации правоохранительной и судебной деятельности.

Ключевые слова: цифровые технологии, электронное доказательство, электронное правосудие, уголовное судопроизводство, цифровизация процессов в сфере уголовного правосудия

INFORMATION TECHNOLOGIES IN CRIMINAL PROCEEDINGS: PROBLEMS OF REGULATORY REGULATION

Abstract. The article deals with the issues of regulatory regulation of the use of information technologies in the field of criminal proceedings based on the analysis of existing international acts and national legislation. The study concluded that it is necessary to develop and legislate the concepts of “electronic justice”, “electronic evidence” in order to ensure the rights and freedoms of participants in criminal proceedings, improve access to justice and modernize law enforcement and judicial activities.

Keywords: Information technologies, Electronic evidence, Electronic justice, Criminal proceedings, Digitalization of criminal justice processes

Современная трансформация уголовного судопроизводства требует внедрения новых технологий и информационных процедур в целях обеспечения доступа к эффективному и доступному правосудию. Применение подобных технологий требует высокого уровня проработанности правового материала, чтобы нивелировать угрозу злоупотребления цифровыми технологиями и обеспечить соблюдение прав и свобод человека в цифровую эпоху. Для этих целей требуется анализ действующих международных правовых стандартов в данной сфере, исследование механизмов и принципов применения электронных технологий, а также выявление противоречий, коллизий, пробелов и модернизация законодательства и правового инструментария.

В настоящее время основным международным актом в сфере регулирования цифровых технологий является «Окинавская хартия глобального информационного общества» [1], принятая в 2000 г., которая является основой для разработки национального законодательства стран-участников в сфере интернет – технологий. Хартия закрепила необходимость формирования и развития информационного сообщества на основе информационно-коммуникационных технологий в качестве залога стабильного и взаимовыгодного прогресса; признание ведущей роли цифровых технологий в разрешении глобальных социальных и экономических проблем и обязательства государств-участников Хартии способствовать развитию информационного пространства.

Резолюция Генеральной Ассамблеи ООН A/RES/55/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [2], детализирует отдельные положения Окинавской хартии и отмечает положительную динамику развития информационных технологий и перспективы для налаживания и расширения международного сотрудничества в сфере информационной безопасности.

В итоговых решениях Организации Объединенных Наций по проблемам предупреждения преступности и уголовного правосудия неоднократно затрагивались

проблемы разработки эффективных принципов, средств и методов противодействия киберпреступности, преступлениям с использованием новых цифровых технологий и указывалось на необходимость разработки правовых механизмов противодействия такого рода преступлениям, в том числе путем применения новых процессуальных и криминалистических средств, а также новых подходов к правовому регулированию и нормативному закреплению использования современных цифровых технологий в процессе раскрытия, расследования, рассмотрения и разрешения уголовного дела, а также в целях предупреждения совершения преступлений.

Нормативные основы использования цифровых возможностей противодействия преступности в Российской Федерации закреплены в законе «Об информации, информационных технологиях и о защите информации», который определяет содержание понятий: «информационные технологии», «информационная система», «электронный документ», «электронное сообщение» и др.; устанавливает основные принципы правового регулирования отношений в сфере информационных технологий; регулирует порядок применение информационных технологий в целях идентификации физических лиц [4], однако необходимо отметить, что содержание данных категорий носит общий характер и не отражает специфики уголовно-процессуальной деятельности.

Федеральный закон «О персональных данных» закрепляет принципы и правила сбора и обработки персональных данных, а также законодательно определяет понятие «персональных данных» и «биометрических персональных данных», их обработки, распространения, блокировки, обезличивания и уничтожения [5], что является основой для дальнейшего нормативного урегулирования вопросов использования персональных данных при производстве оперативно-розыскных мероприятий и расследования и разрешения уголовных дел.

Принятая в 2019 г. «Концепция информационной политики судебной системы на 2020–2030 годы» определила в качестве цели – открытость и гласность судопроизводства и обеспечение доступа граждан и организаций к информации о деятельности судов на основе принципа безопасности информационных баз судов и охраны персональных данных. Концепция направлена на дальнейшее развитие и совершенствование системы ГАС «Правосудие», предусматривает формирование единого информационного пространства судебной системы, результатом которого является совершенствование нормативного регулирования информационных ресурсов судебных органов [6].

Развитие информационных и электронных технологий позволило внедрить в процесс расследования и рассмотрения уголовных дел смс-информирование участников уголовного судопроизводства о дате и времени производства следственных действий и судебных заседаний; применения электронных браслетов для обеспечения соблюдения условий такой меры пресечения как домашний арест, который длительное время не применялся в уголовном судопроизводстве в виду отсутствия технических средств слежения за подозреваемым и обвиняемым.

В настоящее время в УПК РФ закреплена возможность использования систем видеоконференцсвязи при производстве отдельных следственных действий: допроса, очной ставки и опознания; определен процессуальный порядок изъятия

электронных носителей информации; предусмотрена выдача исполнительного листа в форме электронного документа, который заверяется усиленной квалифицированной электронной подписью судьи.

Кроме того, уголовно-процессуальный закон разрешает подачу в форме электронного документа, заверенного электронной подписью, ходатайств, заявлений, жалоб и представлений в суд и применение видеоконференцсвязи в ходе судебного разбирательства [3]. Однако, в отличие от зарубежного процессуального законодательства, УПК РФ не содержит определения «электронные доказательства», критериев допустимости, относимости и достоверности цифровых доказательств, а в сфере уголовной юстиции не создана и не функционирует в полной мере система электронного документооборота. Подобный подход к нормативному регулированию применения цифровых технологий в уголовном судопроизводстве затрудняет реализацию концепции электронного правосудия, носит фрагментарный характер регулирования, свидетельствует об отсутствии системности нормативного регулирования.

В целях преодоления указанных проблем, по нашему мнению, требуется разработка и законодательное закрепление в процессуальных актах следующих понятий:

1) электронный документ;

2) требования к электронному документу как процессуальному доказательству;

3) цифровая информация;

4) требования к источникам цифровой доказательственной информации;

5) электронное доказательство;

6) основания и порядок получения электронного доказательства;

7) электронное уголовное дело;

8) критерии допустимости, относимости и достоверности цифровых доказательств.

Таким образом, в настоящее время требуется законодательное регулирование требований к защите информации при использовании информационных систем в процессе расследования уголовного дела; к проведению онлайн процессов; к процессуальным процедурам применения цифровых технологий; к техническому обеспечению процесса расследования и рассмотрения уголовного дела.

Список литературы

1. Окинавская Хартия глобального информационного общества // Дипломатический вестник. 2000. № 8.

2. Резолюции A/RES/55/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27 20 (дата обращения: 11.09.2022).

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 14.07.2022, с изм. от 18.07.2022) // СПС «КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=422078 (дата обращения: 18.09.2022).

4. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) // СПС

«КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=422054& (дата обращения: 18.09.2022).

5. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) // СПС «КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=422241 (дата обращения: 18.09.2022).

6. Концепция информационной политики судебной системы на 2020–2030 годы (одобрена Советом судей РФ 05.12.2019) // СПС «КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=339776 (дата обращения: 18.09.2022).

Ю. Ю. Малышева,
кандидат юридических наук, доцент,
заведующий кафедрой
уголовного права и криминологии,
Казанский институт (филиал) Всероссийского государственного
университета юстиции

УГОЛОВНО-ПРАВОВЫЕ РИСКИ ЦИФРОВИЗАЦИИ ЗДРАВООХРАНЕНИЯ

Аннотация. В статье освещаются основные риски цифровизации здравоохранения, указываются уголовно-правовые риски причинения вреда при передаче персональных данных, требующих обеспечения высокого уровня безопасности. Проблема в настоящее время заключается в отсутствии системы уголовно-правовой защиты персональных данных в России, что логически приводит к уголовно-правовым рискам цифровизации здравоохранения. Цифровизация является основным вектором развития современного российского общества, выступая в роли неотъемлемой российской действительности. Развитие информационных технологий в современной России неминуемо приводит к тому, что они стали использоваться при совершении преступлений. Закономерной реакцией на данные обстоятельства выступают уголовно-правовые меры, способные успешно противостоять данному явлению. Цифровизация здравоохранения включает развитие искусственного интеллекта в здравоохранении, нуждающемся в правильном уголовно-правовом регулировании текущих отношений. Цифровые технологии в здравоохранении необходимо развивать в целях устойчивого прогресса отрасли медицинского права, поскольку цифровизация здравоохранения позволяет решить ряд существенных проблем в условиях пандемии COVID-19.

Ключевые слова*:* цифровизация здравоохранения в уголовном праве, уголовно-правовые риски цифровизации здравоохранения, информационные технологии в уголовном праве, искусственный интеллект в уголовном праве, цифровизация здравоохранения в условиях пандемии COVID-19, уголовно-правовая защита персональных данных в РФ

CRIMINAL AND LEGAL RISKS OF DIGITALIZATION OF HEALTH CARE

Abstract. The article highlights the main risks of digitalization of healthcare, indicates the criminal-legal risks of harm in the transfer of personal data that require a high level of security. The problem currently lies in the lack of a system of criminal law protection of personal data in Russia, which logically leads to criminal law risks of digitalization of healthcare. Digitalization is the main vector of development of modern Russian society, acting as an integral Russian reality. The development of information technologies in modern Russia inevitably leads to the fact that they began to be used in the commission of crimes. A natural reaction to these circumstances is criminal law measures that can successfully counter this phenomenon. The digitalization of healthcare includes the development of artificial intelligence in healthcare, which needs the correct criminal law regulation of current relations. Digital technologies in healthcare need to be developed for the sustainable progress of the medical law industry, since the digitalization of healthcare allows solving a number of significant problems in the context of the COVID-19 pandemic.

Keywords: Gitalization of healthcare in criminal law, Criminal law risks of digitalization of health care, Information technologies in criminal law, Artificial intelligence in criminal law, Digitalization of healthcare in the context of the COVID-19 pandemic, Criminal law protection of personal data in the Russian Federation

Главной гарантией продолжительности и качества жизни человека является его здоровье, поэтому развитие медицины безусловно является ключевым вопросом национальной безопасности. В изменившихся в последнее время условиях жизни человека, при неизбежных обстоятельствах цифровизации нашего общества, вопрос безопасности личности приобрел глобальный масштаб. События, происходящие в мире, наглядно демонстрируют, какое значение имеет здравоохранение для обеспечения национальной безопасности. Инструментом, обеспечивающим предупреждение преступности, правопорядок, безопасность личности и национальную безопасность, является уголовная политика [1. С. 34].

Обеспечение безопасности личности в сфере оказания медицинской помощи предполагает дуалистическую направленность политики противодействия преступности в сфере оказания медицинской помощи.

За время действия Уголовного кодекса РФ, уже более четверти века, существенно изменилось общество, цифровые технологии уверенно вошли в жизнь большинства людей, в особенности в связи с пандемией коронавируса COVID-19, и роль цифровых технологий заметно укрепилась и стала гораздо важнее. Все то, что казалось в XX в. фантастикой, в XXI в. является элементом нормальной повседневной жизни людей.

Таким образом, цифровизация – это актуализация информации, обращающейся в определенной социальной области, в формат, обеспечивающий возможность машинной (компьютерной) обработки данных.

В качестве одной из национальных идей развития цифровых технологий в России на период до 2024 г. указано обеспечение ускоренного внедрения цифровых

технологий в сфере оказания медицинской помощи. Поэтому приведение в соответствие положений уголовного права с глобальной информатизацией преступности является перспективной задачей, которая, безусловно, должна быть решена в ближайшее время. Сформировавшееся в последние годы новые формы преступной деятельности с использованием современных информационно-телекоммуникационных технологий должны получить достойный «ответ» в виде уголовно-правовых императивных методов.

В 1999 году Институтом медицины Национальной академии наук США (NAS) был опубликован отчет «Человеку свойственно ошибаться», в котором отмечено, что врачебные ошибки являются причиной смерти от 44 000 до 98 000 больных ежегодно, что в несколько раз превышает смертность от автомобильных аварий (43 458) и ряда серьезных заболеваний.

В сложившихся условиях важно обеспечить защиту здравоохранения с обеих сторон. По традиции центральным вопросом противодействия преступности в сфере здравоохранения являлось обеспечение безопасности пациента, и, безусловно, значимость этой проблемы нельзя преуменьшать. Вместе с тем, важно обеспечить безопасность и защиту не только пациента, но и медицинского работника. По нашему мнению, защита прав и свобод человека и гражданина не должна носить однобокий характер, обращенный в сторону лишь одного участника правоотношений – пациента. Законодатель должен помнить и о другой стороне этих правоотношений – медицинском работнике. Здесь важно соблюсти такой баланс, чтобы, защищая интересы одной из сторон, не ущемить интересы другой, поскольку, по мнению выдающихся философов, любая дисгармония в отношениях негативно влияет на интересы обеих сторон, и это бесспорно.

В конце XX – начале XXI в. особо остро встала проблема цифровизации здравоохранения.

Цифровизация уголовного права целиком и полностью зависит от аналогичного процесса, происходящего в экономике, поскольку уголовное право современности неизбежно и своевременно старается реагировать на процессы, происходящие в обществе [2. С. 388].

Камнем преткновения в настоящее время является полное отсутствие в России системы защиты персональных данных, по справедливому замечанию Э. Л. Сидоренко, что безусловно отражается на процессе цифровизации здравоохранения.

В октябре 2019 г. Министерством здравоохранения Российской Федерации был утвержден Федеральный проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ «Цифровой контур здравоохранения») на период 2019–2024 годов» (далее – ЕГИСЗ). Настоящий проект призван решать задачи по трансформации процессов организации системы здравоохранения.

Примечательным является то, что в России в 2020 г. в цифровое здравоохранение было вложено 47,3 млн долл., в 2021 г. уже 50,2 млн долл. Самыми популярными направлениями у инвесторов этой сферы в России стали– телемедицина, мобильные приложения, сервисы для пациентов, медицинское страхование, а также особое место занимают решения с использованием искусственного интеллекта.

С активным развитием искусственного интеллекта в сфере здравоохранения возникают вопросы, касающиеся правовой оценки действия систем и тех, кто будет нести ответственность в случае причинения вреда. С одной стороны системы искусственного интеллекта способны к самообучению (система способна сама принять решение о совершение действия, которое может квалифицироваться как преступление) с другой стороны указанные системы функционирует посредством деятельности конкретного физического лица. Необходимо учитывать, что в основе функционирования искусственного интеллекта находится производитель продукта и разработчик, которые могут нести ответственность за выполнение работ и оказание услуг, не отвечающих требованиям безопасности жизни или здоровья потребителя. Не исключено, что в деятельность системы может вмешаться иное лицо со стороны и заразить вирусом, изменить исходный код, перепрограммировать систему. В этом случае имеет место совокупность преступлений в сфере компьютерной безопасности и преступлений против личности. В сфере применения искусственного интеллекта отсутствует объективная статистика, поэтому чтобы лица, использующие информационные системы для совершения преступления не могли избежать юридической ответственности необходимо совершенствование всего российского законодательства, в том числе и уголовного.

Цифровая экосистема здравоохранения должна обеспечивать беспрепятственный и безопасный обмен медицинскими данными между пользователями, поставщиками медицинских услуг, менеджерами систем здравоохранения и службами медицинских данных.

В цифровой стратегии особая роль отводится медицинским данным, которые классифицируются как конфиденциальные персональные данные или личная идентифицируемая информация, требующая высокого уровня безопасности.

Активность киберпреступников в отношении медицинских учреждений с каждым годом растет. В 2021 г. самой атакуемой отраслью года было здравоохранение, а к 2022 г. медицина входит в тройку лидеров по количеству разного рода кибератак. Уже в начале мая 2022 г. Президент России Владимир Путин подписал указ о создании отдельной кибербезопасности на объектах критической информационной инфраструктуры, включая учреждения здравоохранения. Поэтому в рамках уголовно-правовой политики совершенствование правового регулирования предупреждения преступности происходит за счет концентрации внимания на изменении норм уголовно-правового законодательства и практики его применения [3. С. 65].

Для того, чтобы не стать жертвой уголовных преступлений, совершенных с помощью информационных технологий, следует не только быть осведомленным в алгоритме действий при взаимодействии с правоохранительными органами, но и применять определенные превентивные меры. Несмотря на существование широкого пласта возможностей для противодействия преступлениям с использованием информационных технологий, большинство экспертов склоняются к мнению, что превентивные меры являются наиболее эффективным способом борьбы с киберпреступлениями.

Список литературы

1. Лопашенко Н. А. Уголовная политика. Москва: ВолтерсКлувер, 2009. С. 34.
2. Малышева Ю. Ю. К вопросу о цифровизации уголовного права в тандеме с цифровой экономикой // Вектор развития управленческих подходов в цифровой экономике: материалы III Всероссийской научно-практической конференции. Казань, 2021. С. 387–393.
3. Малышева Ю. Ю. Мнимая криминализация и уголовная политика: актуальные вопросы // Сборник материалов VIII Международной научно-практической конференции. Санкт-Петербург, 2020. С. 64–67.

Н. В. Машинская,
кандидат юридических наук, доцент,
Северный (Арктический) федеральный университет
имени М. В. Ломоносова

ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ ДОПРОСА, ОЧНОЙ СТАВКИ И ОПОЗНАНИЯ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ

Аннотация. Включение в Уголовно-процессуальный кодекс Российской Федерации ст. 189.1, предусматривающей проведение в ходе предварительного расследования допроса, очной ставки и опознания путем использования систем видеоконференцсвязи, вызвало дискуссии среди теоретиков и практикующих юристов относительно обеспечения доказательственного значения получаемого результата и обеспечения прав участников процесса. В настоящем исследовании на основе анализа законодательного регулирования и мнений различных авторов формулируется вывод о необходимости совершенствования рассматриваемой нормы.

Ключевые слова: участники уголовного судопроизводства, следственные действия, доказательства, принципы уголовного судопроизводства, видеоконференцсвязь, допрос, очная ставка

PROBLEMS OF LEGISLATIVE REGULATION OF INTERROGATION, CONFERENCE AND IDENTIFICATION USING VIDEO CONFERENCE COMMUNICATION SYSTEMS

Abstract. The inclusion in the Code of Criminal Procedure of the Russian Federation of Article 189.1, which provides for interrogation, confrontation and identification during the preliminary investigation through the use of videoconferencing systems, caused discussions among theorists and practicing lawyers regarding ensuring the probative value of the result obtained and ensuring the rights of participants in the process. In this study, based on the analysis of legislative regulation and the opinions of various authors, a conclusion is made about the need to improve the norm in question.

Keywords: Participants in criminal proceedings, Investigative actions, Evidence, Principles of criminal justice, Video conferencing, Interrogation, Rate

Федеральным законом от 30 декабря 2021 г. № 501–ФЗ в Уголовно-процессуальный кодекс Российской Федерации (далее – УПК РФ) введена новая статья, предусматривающая возможность проведения допроса, очной ставки и опознания путем использования видеоконференцсвязи (далее – ВКС) в ходе предварительного расследования (ст. 189.1 УПК РФ). Ранее закон допускал использование ВКС лишь при допросе свидетеля и только в стадии судебного разбирательства. Апробированный десятилетием опыт и реалии современной действительности (развитие цифровых технологий и постепенное их внедрение во все сферы жизни граждан, появление новой коронавирусной инфекции, большая загруженность органов предварительного расследования) послужили предпосылкой к разработке законопроекта, предлагающего внести изменения в УПК РФ и предоставить следователю и дознавателю право допрашивать потерпевшего, свидетеля, эксперта, специалиста посредством ВКС [1]. В качестве достоинств указанного законопроекта можно отметить четкое определение условий, при наличии которых мог быть осуществлен дистанционный допрос, а также то, что новелла ограничивала процессуальный статус лиц, допрашиваемых при помощи ВКС. Исходя из предлагаемой нормы, в таком формате не могли допрашиваться подозреваемый и обвиняемый. Наряду с этим в законопроекте имелись недостатки, например, отсутствие указаний на порядок проведения видеозаписи и требований к ней. В то же время, такой регламентации не содержит и ст. 278.1 УПК РФ, которая применяется в судах повсеместно, при этом никаких нареканий с точки зрения обеспечения прав участников уголовного судопроизводства, упомянутая норма не вызывала. Юридическое сообщество позитивно отреагировало на предлагаемый законопроект, считая его нацеленным на реализацию принципа разумного срока уголовного судопроизводства, всестороннего, полного и объективного исследования обстоятельств уголовного дела, что в итоге позволит повысить качество предварительного расследования [4. С. 125–136; 6. С. 25–28; 7. С. 159–165].

Однако предлагаемая новелла была одобрена и вступила в действие в иной редакции (ст. 189.1 УПК). Во-первых, обращает на себя внимание то обстоятельство, что законодатель, помимо допроса, допускает проведение посредством ВКС так же очной ставки и опознания, то есть тех следственных действий, которые по своей цели, уголовно-процессуальной характеристике и организации существенно отличаются от допроса, являются наиболее сложными, требующими для проведения специальной технической и тактической подготовки. Во-вторых, в новелле не нашли отражения условия, при наличии которых перечисленные следственные действия могут быть проведены посредством ВКС. В-третьих, рассматриваемая норма не ограничивает процессуальный статус лица, с участием которого проводится допрос, очная ставки или опознание. Учитывая, что предварительное расследование нацелено на сбор доказательственной базы по уголовному делу, обращение к вопросу об использовании технических каналов связи при проведении следственных действий является весьма актуальным с точки зрения обеспечения допустимости полученных результатов и прав участников уголовного судопроизводства. Представляется, что редакция состоявшейся нормы, содержащейся в ст. 189.1 УПК РФ, неизбежно повлечет различного рода затруднения в применении.

Уголовно-процессуальный закон не обязывает правоприменителя испрашивать согласие участников уголовного процесса на проведение допроса, очной ставки или опознания путем применения ВКС. Руководствуясь соображениями процессуальной самостоятельности, следователь, дознаватель (далее используется обобщающее понятие – «следователь») вправе сам решать каким образом проводить следственное действие. Он обязан лишь соблюсти общее правило УПК РФ и уведомить участников следственного действия о его проведении с использованием технических средств, а также сделать об этом отметку в протоколе следственного действия, удостоверив ее подписью участника (ч. 6 ст. 164 УПК РФ). Сложившаяся ситуация способна существенно нарушить права участников со стороны защиты, которые лишены возможности возразить против проведения опознания таким способом. Между тем, именно в ходе предъявления лица для опознания проблема обеспечения прав подозреваемого, обвиняемого возникнет особенно остро. Допустимость результата предъявления для опознания зависит от ряда факторов. Во-первых, от того, насколько хорошо подобраны лица, предъявляемые для опознания. Чем больше они схожи по возрасту, росту, цвету волос, одежде и т. п., тем достовернее сведения, полученные от опознающего. В то же время удаленное проведение предъявления лица для опознания, в особенности при недостаточно хорошем качестве связи, не позволит опознающему узнать опознаваемого по росту, голосу, чертам лица либо приведет к ошибке, что так же имеет пагубное значение для установления истины по уголовному делу. Во-вторых, от того, насколько качественно организовано опознание, насколько опознающий независим от мнения следователя или оперативного сотрудника, как правило, сопровождающего следственное действие. При дистанционном формате проведения опознания проконтролировать и исключить какие-либо подсказки со стороны заинтересованного в раскрытии преступления лица, окажется невозможным в силу того, что при проведении опознания посредством ВКС, защитник подозреваемого, обвиняемого и опознающий будут находиться по разные стороны видеомоста. При этом закон обязывает осуществлять только запись видеосвязи, а что происходит за пределами видимости камер останется незамеченным (ч. 4 ст. 189.1 УПК РФ). Отсутствие требований к порядку проведения ВКС, например, каким образом должна быть установлена камера относительно опознаваемых, должна ли она охватывать сразу всех опознаваемых или демонстрировать каждого по отдельности, как часто можно или нужно «наводить» экран на опознаваемых и т. п. так же породят сомнения относительно добросовестности организации и проведения следственного действия, создаст условия для оспаривания его результатов. Кроме того, дистанционное опознание затрудняет реализацию прав защитника: заявление ходатайств, принесение замечаний на протокол следственного действия и т. п. Аналогичные вопросы возникнут при предъявлении для опознания предмета или документа.

Такой же сомнительный доказательственный материал будет формироваться в результате проведения очной ставки путем ВКС. Цель очной ставки заключается в устранении противоречий в показаниях ранее допрошенных лиц. Достижение цели следственного действия обеспечивается возможностью, в том числе, задавать вопросы участникам очной ставки друг другу. Важнейший психологический аспект

очной ставки заключается в том, что в ходе очной ставки, ее участники находятся друг напротив друга и далеко не каждый способен давать ложные показания, глядя в глаза участнику следственного действия. Использование ВКС для проведения очной ставки нивелирует ее психологическое значение и фактически превращает в обычный дистанционный допрос.

Современная редакция УПК РФ не содержит каких–либо ограничений по статусу лица, которого можно допрашивать в ходе предварительного расследования дистанционно. Представляется, что таким образом, можно допрашивать лишь потерпевших, свидетелей, экспертов и специалистов. Хотя в юридической литературе встречаются и другие мнения [5. С. 111–122]. Думается, что возможности следователя в применении ВКС при допросе будут существенно ограничены, если допрашиваемым окажется малолетний, лицо с психическими или физическими недостатками, лицо в преклонном возрасте. Отдельному осмыслению подлежит вопрос о реализации следователем права на демонстрацию допрашиваемому в ходе допроса вещественных доказательств. Проведение дистанционного допроса существенно снижает возможности следователя по установлению таким способом фактических обстоятельств, имеющих значение для уголовного дела. Думается, что для реализации такого права в ходе допроса по ВКС требуется дополнительное нормативное регулирование, которое бы регламентировало порядок предъявления допрашиваемому вещественных доказательств, иных документов, их исследование и отражение процессуального действия в протоколе. В противном случае, следователю придется от них отказаться.

Результаты научно-технического прогресса, безусловно, должны быть использованы в сфере уголовного судопроизводства, однако их использование не должно ставить под сомнение доброкачественность собранных по уголовному делу доказательств, содержать угрозу нарушения прав участников процесса, подрывать авторитет правосудия. Достижение задач уголовного судопроизводства должно обеспечиваться детальным правовым регулированием. В связи с этим полезно обратиться к зарубежному опыту. Так, например, ст. 224.1 УПК Республики Беларусь, предоставляя следователю право провести допрос, очную ставку и опознание посредством ВКС, ограничивает круг допрашиваемых потерпевшим и свидетелем, а также содержит условия, при которых норма реализуется. В частности, посредством ВКС допрос, очная ставка и опознание могут проводиться только, когда необходимо обеспечить безопасность участнику процесса, достичь быстрого, всестороннего и полного исследования обстоятельств дела. Наряду с этим обязательным требованием является обеспечение всех прав участников следственного действия, а также надлежащее качество изображения и звука [2]. А ст. 213 УПК Республики Казахстан предусматривает возможность проведения допроса свидетеля и потерпевшего посредством ВКС не только по инициативе следователя, но и по ходатайству сторон [3].

Таким образом, анализируемая норма нуждается в совершенствовании. Представляется, что в ходе предварительного расследования с использованием ВКС может проводиться только допрос потерпевшего, свидетеля, эксперта и специалиста. Наряду с этим в норме, регламентирующей его проведение, необходимо закрепить требование к качеству ВКС, а также право участников процесса возражать против проведения допроса в таком формате.

Список литературы

1. Законопроект № 434998–7 «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации». URL: http://asozd2c.duma.gov.ru/addwork/scans.nsf/ID/BAE69922D1C0B01B43258266005F6F81/$FILE/434998–7_05042018_434998–7.PDF? OpenElement (дата обращения: 31.08.2022).

2. Уголовно-процессуальный кодекс Республики Беларусь. URL: https://kodeksy-by.com/ugolovno-protsessualnyj_kodeks_rb/224–1.htm (дата обращения: 04.09.2022).

3.Уголовно-процессуальный кодекс Республики Казахстан. URL: https://online.zakon.kz/document/?doc_id=31575852&pos=4;-106#pos=4;-106 (дата обращения: 05.09.2022).

4. Антонович Е. К. Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств) // Актуальные проблемы российского права. 2019. № 6. С. 125–136.

5. Бондарцева О. Г. Дистанционное участие обвиняемого (подозреваемого) на стадии предварительного расследования как альтернатива приостановлению производства по уголовному делу // Актуальные проблемы российского права. 2021. № 10. С. 111–122.

6. Плетникова М. С., Семенов Е. А. К вопросу использования видеоконференцсвязи при производстве допроса // Вестник Уральского юридического института МВД России. 2021. № 1. С. 25–28.

7. Поддубняк А. А., Евдокимова Е. С. Допрос свидетеля посредством видеоконференцсвязи на стадии предварительного расследования как новелла российского законодательства // Ученые записки Крымского федерального университета имени В. И. Вернадского Юридические науки. 2018. Т. 4 (70), № 3. С. 159–165.

С. В. Мурадян,
кандидат юридических наук, заместитель начальника кафедры,
Московский университет Министерство внутренних дел
Российской Федерации им. В. Я. Кикотя

СУЩНОСТЬ И ОСОБЕННОСТИ ПРАВОВОЙ ПРИРОДЫ ЦИФРОВЫХ АКТИВОВ В РОССИИ КАК ПРЕДМЕТА ХИЩЕНИЯ

Аннотация. В статье анализируется сущность и особенности правовой природы различных видов цифровых активов, приобретающих все большую популярность по всему миру в условиях цифровизации экономики. Обладая существенными преимуществами, одновременно, они представляют собой высокорисковые инструменты, причем, как с финансовой, так и с правовой точек зрения. Противоречивые подходы к правовому регулированию блокчейн в разных странах, а также диссонанс в употреблении терминов приводит к большому количеству пробелов в правовом регулировании оборота цифровых активов и не позволяет сформировать эффективную систему способов защиты права собственности на них и обеспечить безопасность

их оборота уголовно-правовыми средствами. Целью данной статьи является рассмотрение проблем использования понятийно-категориального аппарата в сфере оборота цифровых активов в российском законодательстве, оценка особенностей режима правового регулирования оборота различных видов цифровых активов в Российской Федерации, а также разработка предложений по обеспечению режима должной уголовно-правовой охраны цифровых активов, устранению препятствий признания их предметом преступления путем приведения в соответствие понятийно-категориального аппарата гражданского и уголовного права в рассматриваемой сфере.

Ключевые слова: цифровая экономика, цифровые активы, токен, цифровое право, цифровые утилитарные права, цифровые финансовые активы, цифровая валюта, криптовалюта, биткоин, цифровой рубль, виртуальные активы, виртуальная валюта, виртуальное имущество, ICO, хищение, мошенничество

THE ESSENCE AND PECULIARITIES OF THE LEGAL NATURE OF DIGITAL ASSETS IN RUSSIA AS AN OBJECT OF EMBEZZLEMENT

Abstract. The article analyzes the essence and peculiarities of the legal nature of various types of digital assets, which are becoming increasingly popular around the world in the context of digitalization of the economy. Having significant advantages, at the same time, they are highly risky instruments, both financially and legally. Contradictory approaches to the legal regulation of blockchain in different countries, as well as the dissonance in the use of terms leads to a large number of gaps in the legal regulation of digital assets turnover and does not allow to form an effective system of ways to protect their ownership rights and ensure the safety of their turnover by criminal law means. The purpose of this article is to consider the problems of using the conceptual and categorical apparatus in the field of digital assets turnover in the Russian legislation, the assessment of the peculiarities of the legal regulation of the turnover of various types of digital assets in the Russian Federation, as well as the development of proposals to ensure the regime of proper criminal law protection of digital assets, removing obstacles to their recognition as a subject of crime by bringing in line the conceptual and categorical apparatus of civil and criminal law in this area.

Keywords: Digital economy, Digital assets, Token, Digital law, Digital utility rights, Digital financial assets, Digital currency, Cryptocurrency, Bitcoin, Digital ruble, Virtual assets, Virtual currency, Virtual property, ICO, Embezzlement, fraud

Цифровые активы, будучи новыми объектами имущественных экономических отношений, существующими в информационно-телекоммуникационной сети Интернет, являются на данный момент основным инструментом цифровой экономики, подверженным значительным рискам. Критически важным условием развития цифровой экономики в России становится обеспечение уверенности всех экономических субъектов в своей защищенности в цифровом пространстве. Этого можно добиться, в первую очередь, за счет формирования и развития нормативно-правовой базы, обеспечивающей реализацию механизмов противодействия преступлениям в сфере оборота цифровых активов.

Появившиеся в ходе законодательной трансформации в условиях цифровизации расслоения в гражданско-правовой и уголовно-правовой терминологии существенно снизили возможности правоохранительной системы по минимизации таких рисков, равно как и их последствий. Еще в 1999 г. Конституционный Суд Российской Федерации указал, что неопределенность содержания правовой нормы, допускает возможность неограниченного усмотрения в процессе правоприменения и неизбежно ведет к произволу, а значит – к нарушению принципов равенства, а также верховенства закона [29].

Так, термин «имущество» в уголовном судопроизводстве приобрел особенность, отличающую его от базового понимания с гражданско-правовой точки зрения, а понятие «право на имущество» и вовсе отсутствует в гражданском праве. Следует согласиться с позицией К. В. Ображиева, что уголовное право требует «унифицированного» подхода в реформировании, что подразумевает смену имеющейся дифференциации предмета корыстных имущественных преступлений (имущество и право на имущество) и установление в УК РФ такого режима уголовно-правовой охраны имущества, который бы совпадал с его гражданско-правовым пониманием [17].

Цифровые активы включают с учетом корреляции понятий, используемых российским законодателем и общепринятых в IT-терминологии, виртуальные активы, т. е. активы, непосредственно созданные в распределенных реестрах, а также токенизированные цифровые активы, существующие в реальном выражении, права на которые помещены в цифровую среду. Подобная классификация важна, в первую очередь, именно для определения правового статуса каждого из них и возможных мер защиты в том числе с позиции уголовного законодательства.

Реально существующие токенизированные активы с точки зрения оценки рисков, намного позитивнее воспринимаются государствами, чем созданные непосредственно в распределенных реестрах, за счет большей безопасности при их обороте. Это подтверждается и мнением экспертов Базельского комитета по банковскому надзору, которые в июне 2021 г., призывая, анализировать природу конкретного криптоактива при установлении значения риска, классифицировали их на три группы. Наименьшими рисками при этом обладают материальные и нематериальные активы группы 1а, включающей традиционные активы, отображенные в форме токенов [25]. Безусловно, речь здесь идет о финансовых рисках, которые в том числе являются частью риск-ориентированного подхода в сфере противодействия преступлениям, совершаемым по поводу, в отношении или с использованием цифровых активов.

Унификация подходов к правовой регламентации статуса новых объектов экономических отношении, наименования которых появились из IT-терминологии – это новый тренд в области права, обусловленный появлением и развитием цифровой экономики. Разработка правовых режимов обеспечения защиты таких объектов продиктована неизбежным расширением средств выражения и сохранения стоимости в информационно-телекоммуникационной сети [19]. К таким объектам и относится «токен».

По сути, токен представляет собой способ фиксации прав в цифровой форме. Существуя в виде цифровой записи в регистре на блокчейн-платформе и выполняя

разнообразные функции, токен как достаточно гибкий цифровой (в первую очередь, финансовый) инструмент дает возможность участникам цифрового гражданского оборота совершать в киберпространстве определенные (цифровые) действия (транзакции), прежде всего цифровые «сделки» [11]. Правовое регулирование блокчейн в разных странах идет совершенно по-разному пути. В мире существует устоявшая классификация токенов. Но в целом одни и те же токены в одной стране могут признаваться служебными токенами, а в то же время в другой, инвестиционными.

При попытке урегулирования оборота таких объектов Российская Федерация, исходя из традиций построения правовой системы в нашей стране, пошла по своему собственному пути, переименовав «токен» в «цифровое право». По сути, оно не является новым объектом права, а, как и токен представляет собой новую форму фиксации существующих прав. То есть в российском законодательстве сущность цифрового права близка к сущности ценной бумаги.

Придерживаясь позиции выработки унифицированной терминологии в рамках действующего законодательства, можно утверждать, что удостоверенные токенами права на объекты гражданских прав, представляя собой цифровые права, могут быть защищены гражданско-правовыми способами, и одновременно, в случае посягательства на них, могут быть признаны предметом хищений в уголовном праве. Соотнесем существующие токены с цифровыми правами в соответствии со ст. 141.1 ГК РФ [1].

Вступивший в силу с 01.01.2020 Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменении в отдельные законодательные акты Российской Федерации» ввел понятие утилитарных цифровых прав [6]. Предполагалось, что они должны быть точной копией служебных токенов. Но по смыслу закона получается, что последние могут быть приравнены к утилитарным цифровым правам только, если созданы на платформе, отвечающий всем стандартам вышеназванного Федерального закона. Получается, что в случае, если компания в любой точке мира отказывается произвести такие изменения, которые от нее требует Федеральный закон Российской Федерации, то права лица, имеющего токены, в рамках такой цифровой платформы защите на территории Российской Федерации не подлежат.

Согласно Федеральному закону от 31.07.2020 № 259-ФЗ (ред. от 14.07.2022) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» еще одним видом цифровых прав в России признаются цифровые финансовые активы [9], т. е. есть инвестиционные токены. Они могут быть представлены денежными требованиями к эмитенту, а также представлять собой право участия в капитале непубличного акционерного общества и права по эмиссионным ценным бумагам, включая требования их передачи. На мой взгляд ситуация с данным видом токенов наиболее понятна. Уголовно-правовая охрана таких объектов может строиться, исходя из имеющейся практики противодействия преступлениям, совершаемым на рынке ценных бумаг.

На данный момент Банк России зарегистрировал три платформы, которые могут выпускать подобные активы в обращение: Atomyze, «Сбербанк» и Lighthouse. А вот обеспечивать заключение сделок с цифровыми финансовыми активами (об-

мен, покупка, продажа, погашение) могут лишь компании из реестра операторов обмена, который будет вести Центральный Банк России. Однако на данный момент ни один такой оператор обмена в реестре не числится.

Весьма сомнительной представляется позиция законодателя согласно пояснительной записке к законопроекту от 26.03.2018 № 424632–7 «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» о том, что цифровые права необходимо регулировать, как «важную для экономики сущность», а «бонусы, виртуальные предметы и т. п. не надо, поскольку они не имеют существенного значения для экономики» [19]. В случае с бонусами речь идет о так называемых «токенах-вознаграждения». В последнее время все большую популярность приобретают маркетплейсы, которые активно используют подобные токены вместо так называемых «баллов за лояльность». Таким образом, пропадает страх потерять карту лояльности, а у интернет-площадок появляется возможность токенизировать свой бизнес, воспользовавшись всеми преимуществами блокчейн-технологий.

Существуют также токены-пожертвования – это просто своеобразные баллы без каких-либо обязательств и функциональной нагрузки. Они начисляются за пожертвования в пользу проекта.

Можно сделать вывод, что часть служебных токенов, токены-вознаграждения и токены-пожертвования законодателем не отнесены к категории цифровых прав, что весьма странно, учитывая, что в пояснительной записке к вышеупомянутому законопроекту от 26.03. 2018 № 424632–7 вводится базовое понятие «цифровое право» вместо термина «токен» в новом современном его значении, как шифр, владение которым дает в сети определенные возможности [19].

Предполагаю, что подобное решение обусловлено, в том числе и тем, что токены-вознаграждения и токены-пожертвования не открывают доступ к функционалу блокчейна и не дают права собственности на что-либо, поэтому законодатель их «обошел» при конструировании понятия «цифрового права».

При пристальном изучении можно сказать, что подход российского законодателя схож с международным. Наиболее близкой к внедренной в российскую правовую систему классификации «цифровых прав» является классификация токенов, разработанная Комиссией по ценным бумагам и биржам США (SEC) и Службой по надзору за финансовыми рынками Швейцарии (FINMA). Интеграция позиции FINMA, направленной на оценку экономической функции токена, с позицией SEC, основанной на оценке степени родства токена с ценными бумагами, позволила классифицировать их на: платежные токены или криптовалюты, токены – активы или инвестиционные токены (токены безопасности) и потребительские (служебные) токены [21].

Виртуальные активы включают в себя криптовалюты (согласно российскому законодательству, цифровые валюты) и другие токены оплаты, токены созданные путем ICO (Initial Coin Offering – первичного размещения токенов с целью привлечения инвестиции для развития проекта).

Согласно позиции Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) виртуальные активы являются средством цифрового выражения сто-

имости, которое может торговаться или переводиться цифровым образом и может быть использовано для целей платежей или инвестиции. При этом они не включают в себя средства цифрового выражения фиатных валют, ценных бумаг и других финансовых активов [16].

Такое выделение цифровых валют центральных банков государств из общего концепта регулирования вполне объяснимо, учитывая совершенно другую природу данного инструмента и возможных рисков. Так, например, создаваемый в России цифровой рубль существенно отличается от иных виртуальных активов. Во-первых, согласно Докладу для общественных консультаций Банка России цифровой рубль выполняет все функции денег, являясь средством обращения, платежа, мерой стоимости и средством сбережения. Во-вторых, он имеет эмитента, гарантирующего надежность и ответственность процесса выпуска и обращения цифрового рубля. В-третьих, цифровой рубль – это обязательство государства, стоимость которого эквивалента наличной и безналичной форме рубля [24].

Все возрастающие масштабы использования криптовалют, сопряженные с высокими рисками их применения для отмывания доходов, финансирования терроризма, финансирования распространения оружия массового уничтожения, а также для обслуживания теневого сектора экономики, потребовали от законодателя разработать публично-правовые установления, в том числе некие требования к обеспечению безопасности соответствующего оборота и с 01 января 2021 г. вступил в силу Федеральный закон от 31.07.2020 № 259-ФЗ, в котором было дано определение «цифровых валют» и сделаны шаги по урегулированию их оборота [9]. Тем не менее все большее число противоречий, возникающих в процессе гражданско-правовой квалификации цифровых валют, а также квалификации противоправных действий с их использованием или в отношении криптовалют дали законодателю основание полагать, что предпринятая попытка была недостаточно плодотворной. Уже в феврале 2022 г. Правительство Российской Федерации утвердило Концепцию законодательного регулирования оборота цифровых валют, в котором признало, что в настоящее время в Российской Федерации отсутствует законодательное регулирование такого высокорискованного финансового инструмента, как цифровая валюта (криптовалюта) [13].

В этой связи вполне закономерно наблюдать следующие позиции судов. Орджоникидзевский районный суд г. Екатеринбурга в своем решении от 14.07.2021 по делу № 2–2582/2021 по делу о взыскании задолженности по договору займа и процентов за пользование займом, предметом которого явились криптовалюты, сделал вывод, что исходя из смысла информационного сообщения Росфинмониторинга «Об использовании криптовалют», использование криптовалют при совершении сделок является основанием для рассмотрения вопроса об отнесении таких сделок (операций) к сделкам (операциям), направленным на легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма [12]. В связи с этим все операции с использованием данного инструмента производятся участниками гражданского оборота на свой риск. При этом судебная защита по их требованиям не предоставляется вне зависимости от того, насколько они являются обоснованными [37].

Криптовалюту нельзя отнести к чисто финансовым активам, поскольку она не является деньгами, а также долевым инструментом другой организации, она не порождает договорного права для владельца получить денежные средства или финансовые активы в будущем и это не договор, расчеты по которому будут или могут быть осуществлены собственными долевыми инструментами [14]. Вместе с тем криптовалюта может быть квалифицирована как объект гражданских прав, так как она способна к обособлению и имеет имущественную ценность, признаваемую оборотом [15]. Анализ имеющейся практики позволяет утверждать, что криптовалюта регулярно выступает предметом обязательств, а также подлежит защите со стороны норм деликтного права. В связи с этим можно согласиться с позицией, что криптовалюту целесообразно относить к «иному имуществу» по смыслу ст. 128 ГК РФ. Надо заметить, что в ряде случаев законодатель, пойдя по пути юридической фикции, для целей конкретных федеральных законов приравнивает криптовалюту к имуществу (ст. 3 Федерального закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [8], ст. 2 Федерального закона от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)» [5], ст. 68 Федерального закона от 02.10.2007 № 229-ФЗ «Об исполнительном производстве» [4], ст. 8 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции») [7].

Распространяя концепцию унифицированного терминологического подхода, можно сделать вывод, что в таком случае криптовалюта может быть признана предметом преступления. Однако в своем решении Волжский районный суд г. Саратова от 14.04.2022 № 2а-1306/2022 указал, что на данный момент в Российской Федерации отсутствует возможность регулирования, в том числе со стороны государства оборота криптовалюты, поскольку она находится вне правового поля и не предоставляет возможность реализации правовых механизмов, в связи с полной децентрализацией процесса выпуска и обращения биткоина [35].

Несмотря на то, что в Российской Федерации с 2014 г. действуют определенные ограничения и запреты в отношении криптовалют, санкции за их нарушение так конкретно и не определены. Хотя цифровые валюты, учитывая их финансовую привлекательность, часто выступают предметом посягательства в хищениях. При этом позиции судов в этом вопросе иногда носят совершенно полярный характер.

Так, в приговоре Солнечногорского городского суда Московской области от 07.10.2020 № 1–227/2020 суд приравнивает криптовалюту к электронным средствам платежа [34]. Хотя, согласно ч. 5 ст. 14 Федерального закона от 31.07.2020 № 259-ФЗ юридические и физические лица в Российской Федерации не вправе принимать цифровую валюту в качестве встречного предоставления за передаваемые ими товары, выполняемые ими работы, оказываемые ими услуги или иного способа, позволяющего предполагать оплату цифровой валютой товаров (работ, услуг) [9].

Совершенно иной позиции придерживается Санкт-Петербургский городской суд, который при рассмотрении апелляционной жалобы П. на приговор Петроградского районного суда г. Санкт-Петербурга от 20.12.2021, которым П. был признан виновным в совершении преступления, предусмотренного п. «б» ч. 3 ст. 161 УК РФ, не согласился с доводами защиты. Защита просила устранить допущенные судом

первой инстанции нарушения уголовно-процессуального закона и исключить из объема обвинения хищение криптовалюты как предмета с отсутствием правового статуса. Санкт-Петербургский городской суд посчитал, что цифровая валюта в виде биткоинов, битшейресов и дигибайтов, похищенных П. и Е., может быть признана имуществом, поскольку использовалась и используется как средство платежа, инвестиций и накопления сбережений, т. е. представляет экономический интерес, а также имеет материальную ценность. Кроме этого, деятельность потерпевшего Ш., была непосредственно связана с управлением криптовалютными счетами и конвертационными действиями с криптовалютами, позволяющими извлекать прибыль из их оборота за пределами РФ и полученный доход, которым, противоправно завладели подсудимые, конвертировать в рубли [30]. Подобные позиции судов позволяют защитить уголовно-правовыми средствами нарушенные права собственников криптовалюты в условиях правовой неопределенности.

Третий кассационный суд общей юрисдикции мнение Санкт-Петербургского городского суда поддержал, указав, что по своей сути основным отличием криптоденег от денег является только способ их возникновения, а поскольку понятие криптовалюты не закреплено законодательно, то следует согласиться с отнесением ее в обвинении, предъявленном осужденным, к «иному имуществу» [32].

Ранее Санкт-Петербургский городской суд уже находил интересный выход из ситуации, где цифровая валюта выступала предметом посягательства. Так, в Апелляционном определении от 20.12.2021 по делу № 1–19/2021, 22–5752/2021 суд указал, что не принимает доводы стороны защиты о том, что биткоин и иные виды криптовалюты не являются предметом вымогательства, поскольку стоимость их не зафиксирована государством, и оборот криптовалюты не регулируется государством, поскольку изначально В. А. вымогал деньги, а криптовалюта была только способом сокрытия перечисления этих денег [31].

К другим токенам оплаты относятся виртуальные валюты. Европейский центральный банк обозначил их, как вид нерегулируемых, цифровых денег, которые выпускаются и обычно контролируются их разработчиками, а также используются и принимаются среди членов определенного виртуального сообщества [28]. По сути, виртуальные валюты предназначены для использования в конкретных виртуальных сферах или мирах, таких, как глобальные многопользовательские онлайн-игры [18].

Несмотря на то, что виртуальная валюта легально не подлежит обмену на фиатную валюту, практика показывает, что предметом посягательства при компьютерном мошенничестве, помимо безналичных и электронных денег, именно виртуальная валюта [23]. Соответственно вопрос урегулирования ее оборота на территории Российской Федерации позволит создать условия для правовой защиты лиц, являющихся собственниками такой валюты.

В судебной практике все чаще встречаются иски, напрямую связанные с массовыми многопользовательскими ролевыми онлайн-играми [20]. Однако судебные решения по ним в Российской Федерации по большей части ограничиваются ссылкой на ст. 1062 ГК РФ и утверждают, что онлайн-игра является игрой в силу определения и целей ее создания, которые указаны в Лицензионном соглашении, а значит к ней подлежит применению ст. 1062 ГК РФ [33], согласно которой не

подлежат судебной защите требования граждан и юридических лиц, связанные с организацией игр или пари и участия в них [2].

Однако встречаются судебные решения, которые рассматривают виртуальные валюты в рамках исков по защите прав потребителей. Так, Лефортовский районный суд г. Москвы признал, что внутриигровая валюта является единицей измерения объема прав использования дополнительного функционала компьютерной онлайн-игры, предоставленного пользователю путем отражения на внутриигровом лицевом счете аккаунта определенного количества единиц измерения прав игрока, которые могут приобретаться как за плату, так и без внесения денежных средств (начислением бесплатно в качестве бонуса за определенные активности в игре, например, участие во внутриигровом аукционе). Однако в этой связи начисленное количество «виртуальной валюты» на внутриигровой счет аккаунта не отражает движение реальных денежных средств между администрацией игры (ответчиком) и владельцем аккаунта [36].

Вопрос урегулирования оборота «виртуального имущества» стоит не менее остро, учитывая, скорость коммерциализации рынка многопользовательских онлайн-игр. «Виртуальное имущество» в основе своей представляет собой всего лишь компьютерный код, который направлен преимущественно на имитацию объектов реального (физического) мира в цифровом пространстве. Исключительно виртуальная форма существования таких объектов не мешает осуществлять их обращение, которое затрагивает интересы «реальных» потребителей, поскольку процесс их приобретения и отчуждения основан на явно выраженной потребительской ценности [22].

Рассматривая токен в рамках ICO необходимо оценивать его исключительно, как средство инвестирования, а последующий оборот таких токенов требует разработки самостоятельных правил. Финансирование для бизнес-проектов привлекается через выпуск и размещение среди неограниченного круга инвесторов собственных цифровых активов-токенов в обмен на ликвидную криптовалюту [10], которая в дальнейшем может быть конвертирована в «фиатные» денежные средства. При этом потенциальные риски для вкладчиков здесь максимально велики. Они могут потерять свои активы, как в связи с неблагоприятной финансовой ситуацией, например, в результате провала стартапа, так и в связи с совершением противоправных действий со стороны эмитентов, например мошенничества, когда полученные средства используются не только для целей развития проекта.

Федеральный закон от 02.08.2019 № 259-ФЗ не предусматривает возможности осуществлять инвестирование посредством криптовалют, хотя, в целом, допускает его [6]. В этой связи отсутствие должного правового регулирования приводит к тому, что эмитенты выбирают для реализации ICO-проектов иностранные юрисдикции с прозрачной законодательной позицией и благоприятным налоговым режимом. Однако иностранные государства также стараются всячески урегулировать и обезопасить рынок ICO. Анализ судебной практики США, показывает, что ряд платежных токенов суды США признают ценными бумагами, стремясь распространить на них соответствующее правовое регулирование. Оговариваясь при этом, что вложение денег в криптовалюту, используемую членами децентрализованного сообщества,

функционирующего на основе технологии блокчейн, которая сама управляется этим сообществом пользователей, а не общим предприятием, вряд ли будет считаться ценной бумагой в соответствии с известным тестом, изложенным в S.E.C. против W. J. Howey Co., 328 U.S. 293, 298–99 (1946) [26]. Однако в ряде случаев, когда эмитенты предпринимают попытки избежать федеральных законов США о ценных бумагах, маркируя свой продукт криптовалютой или цифровым токеном, такие действия лиц признаются незаконными и эмитентов обязуют вернуть денежные средства инвесторам. Так, продажа Telegram и TON 2,9 млрд Граммов 175 покупателям в обмен на 1,7 млрд долл., являются частью более крупной схемы по распределению этих Граммов на вторичном публичном рынке. Учитывая экономические реалии в соответствии с тестом Хоуи, суд США посчитал, что в контексте этой схемы перепродажа Граммов на вторичном публичном рынке является неотъемлемой частью продажи ценных бумаг без обязательного заявления о регистрации [27].

Находящийся на данный момент на доработке проект Федерального закона «Цифровых валютах», разработанный Министерством финансов Российской Федерации, предусматривает легализацию криптовалютной сферы в Российской Федерации, что позволит изменить подход и в вопросах регулирования сферы ICO в России.

Учитывая, что в условиях санкций криптовалюта является одним из наиболее быстрых, удобных и эффективных способов расчета, согласно упомянутому выше законопроекту Минфина России, планируется разрешить оплату внешнеторговой деятельности юридических лиц и предпринимателей за товары, работы, услуги и интеллектуальную деятельность с помощью цифровых валют. Законопроект также предусматривает введение лицензий оператора обмена цифровых валют и оператора цифровой платформы, т. е. в Российской Федерации появится возможность регистрации криптобирж и криптообменников. Однако в рамках законопроекта пока не определены санкции за нарушение предложенного порядка оборота криптовалют и противоправные действия его участников. В целом анализ указанного законопроекта позволяет утверждать, что процесс урегулирования оборота криптовалют в России будет схож с положениями законодательства о регулировании рынка ценных бумаг, т. е. установит достаточно жесткие требования и стандарты.

Список литературы

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 25.02.2022) // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=C3BA75257675D5072BCC4E7ECE908376&mode=splus&rnd=bEJ38g&base=LAW&n=410306#AN2c5ETP7HDTbfU6 (дата обращения: 01.08.2022).

2. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 01.07.2021, с изм. от 08.07.2021) (с изм. и доп., вступ. в силу с 01.01.2022) // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=FCB3B26F22A203831458B5022A803D40&mode=splus&rnd=bEJ38g&base=LAW&n=377025&dst=102595#bCYc5ETs90x4mjI1 (дата обращения: 01.08.2022).

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 14.07.2022, с изм. от 18.07.2022) (с изм. и доп., вступ. в силу с 25.07.2022) // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=cd1d5ETQTfksEs9t&cacheid=E72F48F0F2B9695CE750EC3E9B194479&mode=splus&rnd=bEJ38g&base=LAW&n=422137#0f2d5ETyoIudsejq (дата обращения: 01.08.2022).

4. Федеральный закон от 02.10.2007 № 229-ФЗ (ред. от 14.07.2022) «Об исполнительном производстве» // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=449D73A908B75CBB4B17EA8F2EA896F7&mode=splus&rnd=bEJ38g&base=LAW&n=422117#Zcsi5ETd8dX1zvFA (дата обращения: 08.08.2022).

5. Федеральный закон от 26.10.2002 № 127-ФЗ (ред. от 28.06.2022, с изм. от 21.07.2022) «О несостоятельности (банкротстве)» // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=70FA91E02F524FB53F879EC99BBFD30E&mode=splus&rnd=bEJ38g&base=LAW&n=420507#q9hi5ETnqeSFALa (дата обращения: 08.08.2022).

6. Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=3574F9E534E3295CF57286D2146F42E7&mode=splus&rnd=bEJ38g&base=LAW&n=422183#giik5ET2GqHWqfYA1 (дата обращения: 08.08.2022).

7. Федеральный закон от 25.12.2008 № 273-ФЗ (ред. от 01.04.2022) «О противодействии коррупции» // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=EA714548D7AA19C7C62E5875FA49018A&mode=splus&rnd=bEJ38g&base=LAW&n=413544#Uq1j5ETxLHiU4fYF (дата обращения: 08.08.2022).

8. Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 14.07.2022) «О противодействии легализации (отмыванию) доходов, полученных путем, и финансированию терроризма» // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=F2228864B656A13B2F845BA15CEA0E1D&mode=splus&rnd=bEJ38g&base=LAW&n=422153#yaXi5ET9CaWwtbkP (дата обращения: 08.08.2022).

9. Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 14.07.2022) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=E14508391CB5EC1A9DF3236C4497BB05&mode=splus&rnd=bEJ38g&base=LAW&n=422194#bKfe5ETZtZtV2pdS (дата обращения: 05.08.2022).

10. Аксаков А. Понятие «токен» может быть определено законодательно / 09.12.2017 / Комитет Государственной Думы по финансовому рынку. URL: http://komitet2–12.km.duma.gov.ru/Novosti-Komiteta/item/14060239?ysclid=l6vd095wkt214089722 (дата обращения: 15.08.2022).

11. Василевская Л. Ю. Токен, как новый объект гражданских прав: проблемы юридической квалификации цифрового права / Актуальные проблемы Российского права. 2019. № 5 // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=10CA83176B242C1BEF0354FA266F64E8&mode=splus&rnd=bEJ38g&base=CJI&n=122770#Ucsd5ETQRXn8nRwN 2 (дата обращения: 08.08.2022).

12. Информационное сообщение Росфинмониторинга «Об использовании криптовалют» // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=569654B8A75A572436E 6B 27A04580986&mode=splus&rnd=bEJ38g&base=LAW&n=158661#Teqe5ET0268ebgBn (дата обращения: 05.08.2022).

13. Концепция законодательного регламентирования механизмов организации оборота цифровых валют, утвержденная Правительством Российской Федерации. 08.02.2022 / Правительство России. URL: http://static.government.ru/media/files/Dik7wBqAubc34ed649ql2Kg6HuTANrqZ.pdf (дата обращения: 05.08.2022).

14. Международный стандарт финансовой отчетности (IAS) 32 «Финансовые инструменты: представление» (введен в действие на территории Российской Федерации Приказом Минфина России от 28.12.2015 № 217н) (ред. от 14.12.2020) // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=848D0A4D7FDF20D0993D13EE13A0802B&mode=splus&rnd=bEJ38g&base=LAW&n=374637#prwg5ETCqLhbSNVG (дата обращения: 08.08.2022).

15. Минюст назвал криптовалюту «иным имуществом». URL: https://cryptonews.net/ru/news/regulation/65650/?ysclid=l6vck3v9l8673770654 (дата обращения: 15.08.2022).

16. Обновленное руководство Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) по применению риск-ориентированного подхода в отношении виртуальных активов и провайдеров услуг в сфере виртуальных активов. Октябрь 2021 / Международный учебно-методический центр финансового мониторинга. URL: https://mumcfm.ru/d/ZMaQyboDDRXwu6OnbQGfEFJE8X3HwM82WP5oRyrZ (дата обращения: 08.08.2022).

17. Ображиев К. В. Преступные посягательства на цифровые финансовые активы и цифровую валюту: проблемы квалификации и законодательной регламентации / Журнал российского права. 2022. № 2 // СПС «КонсультантПлюс». URL: https://online3.consulant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=971162C88B3338E8BF5051698B63334D&mode=splus&rnd=bEJ38g&base=CJI&n=141291#V1gd5ETqa0eOTgcw (дата обращения: 08.08.2022).

18. Отчет ФАТФ «Виртуальные активы». Ключевые определения и потенциальные риски в сфере ПОД/ФТ. Июнь 2014 г. / Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма. URL: https://eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf (дата обращения: 08.08.2022).

19. Пояснительная записка к законопроекту № 424632–7 от 26.03.2018 «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского

кодекса Российской Федерации» / Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/bill/424632–7?ysclid=l6ncm2y5pu318025418 (дата обращения: 08.08.2022).

20. Рожкова М. А. Виртуальное имущество и многопользовательская онлайн-игра – как различать возникающие по их поводу отношения? // Закон.ру. 2020. 6 декабря. URL: https://zakon.ru/blog/2020/12/6/virtualnoe_imuschestvo_i_mnogopolzovatelskaya_onlajn-igra__kak_razlichat_voznikayuschie_po_ih_povodu (дата обращения: 05.08.2022).

21. Рожкова М. А. Значимые для целей правового регулирования различия между криптовалютой на базе публичного блокчейна, «криптовалютой» частного блокчейна и национальной криптовалютой / / Хозяйство и право. 2020. № 1 (516). URL: https://elibrary.ru/download/elibrary_41580653_55150735.pdf (дата обращения: 15.08.2022).

22. Русскевич Е. А., Фролов М. Д. Мошенничество в сфере компьютерной информации: монография. Москва: ИНФРА-М, 2020. 147 с. (Научная мысль). С. 19–20.

23. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. Москва: Статут, 2016. 640 с. С. 40.

24. «Цифровой рубль. Доклад для общественных консультаций (октябрь 2020 года)» (утв. Банком России) // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=E857D3D7DAC98A55137DBF16CDDA25F2&mode=splus&rnd=bEJ38g&base=LAW&n=364913#2ETe5ETILns7qxqQ1 (дата обращения: 08.08.2022).

25. Consultative Document of Basel Committee on Banking Supervision. Prudential Treatment of Cryptoasset Exposures. Issued for Comment by 10 September 2021 /The Bank for International Settlements . URL: https://www.bis.org/bcbs/publ/d519.pdf (дата обращения: 08.08.2022).

26. SEC v. W. J. Howey Co., 328 U.S. 293 (1946). / U. S. Supreme Court. URL: https://supreme.justia.com/cases/federal/us/328/293/ (дата обращения: 08.08.2022).

27. United States District Court against telegram Group Inc. and Ton Issuer Inc. Southern district of New York. Case 1:19-cv-09439-PKC from 03/24/20 / Justia Us Law. URL: https://cases.justia.com/federal/district-courts/new-york/nysdce/1:2019cv09439/524448/227/0.pdf?ts=1585128306 (дата обращения: 08.08.2022).

28. Virtual Currency Schemes. ECB Report. October 2012. P. 13 / European Central Bank. URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (дата обращения: 08.08.2022).

29. Постановление Конституционного Суда РФ от 15.07.1999 № 11-П «По делу о проверке конституционности отдельных положений Закона РСФСР «О Государственной налоговой службе РСФСР» и Законов Российской Федерации «Об основах налоговой системы в Российской Федерации» и «О федеральных органах налоговой полиции» // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=E2213FBCE57CDA9D23CD0D2683D98DFC&mode=splus&rnd=bEJ38g&base=LAW&n=23820#C8Od5ETmGsg8kPUs1/ (дата обращения: 05.08.2022).

30. Апелляционное определение Санкт-Петербургского городского суда от 16.05.2022 № 22–2616/2022, 1–257/2021 // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=97DB8B72DCA899C7D5889FF7721CEB2D&mode=splus&rnd=bEJ38g&base=AOSZ&n=5081238#2sej5ETY3DZGLB171 (дата обращения: 08.08.2022).

31. Апелляционное определение Санкт-Петербургского городского суда от 20.12.2021 по делу № 1–19/2021, 22–5752/2021 // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=8BB30E68700B55EA5B0F59C18D4256C8&mode=splus&rnd=bEJ38g&base=AOSZ&n=4878364#kjvj5ETBUjWxl0fD (дата обращения: 08.08.2022).

32. Кассационное определение Третьего кассационного суда общей юрисдикции от 24.06.2021 № 77–1411/2021 // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=C10D4B31598CBB37FEAF6E5C8A378287&mode=splus&rnd=bEJ38g&base=KSOJ003&n=35963#Tfkj5ET46wqfhZ3J (дата обращения: 08.08.2022).

33. Определение Четвертого кассационного суда общей юрисдикции от 01.03.2022 по делу № 88–5695/2022 // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=F31C60CE0A5B986B5B1D27E2386915C6&mode=splus&rnd=bEJ38g&base=KSOJ004&n=72541#SKBk5ETFXl55CyV1 (дата обращения: 08.08.2022).

34. Приговор Солнечногорского городского суда Московской области от 07.10.2020 № 1–227/2020 // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=5EA18D3245367237670AA08F26D4C0BA&mode=splus&rnd=bEJ38g&base=AOKI&n=8961537#mHTj5ETOkQz5RvN81 (дата обращения: 05.08.2022).

35. Решение Волжского районного суда города Саратова от 14.04.2022 по делу № 2а-1306/2022 // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=320749B38EA3DDBD1BB0BF991B4195AF&mode=splus&rnd=bEJ38g&base=AOKI&n=10319504#eeFj5ETxeRh7oZN1 (дата обращения: 05.08.2022).

36. Решение Лефортовского районного суда города Москвы от 09.06.2015 по делу № 2–1619/2015~М-998/2015 // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=17CCF72FEDE8E3A35215CEF4D7EAE3BF&mode=splus&rnd=bEJ38g&base=AOCN&n=4479817#B8Ok5ETUF6RrfQ2j1 (дата обращения: 08.08.2022).

37. Решение Орджоникидзевского районного суда города Екатеринбурга от 14.07.2021 по делу № 2–2582/2021 // СПС «КонсультантПлюс». URL: https://online3.consultant.ru/cgi/online.cgi?req=doc&ts=uk1c5ETWXNyahdpr&cacheid=183F7C58A28644AB4D573FF3D3536288&mode=splus&rnd=bEJ38g&base=AOUR&n=6488711#ZJVg5ETwq0oncIzK (дата обращения: 08.08.2022).

А. А. Нуждин
кандидат юридических наук, доцент,
Академия Федеральной службы исполнения наказаний России

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ КАК ФАКТОР, СПОСОБСТВУЮЩИЙ ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ПО ПРЕДУПРЕЖДЕНИЮ ПЕНИТЕНЦИАРНЫХ ПРЕСТУПЛЕНИЙ

Аннотация. В статье рассмотрены вопросы, связанные с цифровой трансформацией уголовно-исполнительной системы. Сделано предположение о положительном влиянии цифровой трансформации на деятельность по предупреждению пенитенциарных преступлений. Представлены основные нормативные акты, определяющие государственную политику в области цифровой трансформации учреждений и органов уголовно-исполнительной системы. Приведен перечень успешно функционирующих программных систем и комплексов в сфере деятельности уголовно-исполнительной системы.

Ключевые слова: промышленная революция, цифровая трансформация, искусственный интеллект, уголовно-исполнительная система, программные комплексы, предупреждение, преступление

DIGITAL TRANSFORMATION OF THE PENAL ENFORCEMENT SYSTEM AS A FACTOR CONTRIBUTING TO IMPROVING THE EFFECTIVENESS OF ACTIVITIES FOR THE PREVENTION OF PENITENTIARY CRIMES

Abstract. The article deals with issues related to the digital transformation of the penal system. The assumption is made about the positive impact of digital transformation on the prevention of penitentiary crimes. The main normative acts defining the state policy in the field of digital transformation of institutions and bodies of the penal system are presented. The list of successfully functioning software systems and complexes in the field of activity of the penal system is given.

Keywords: Industrial Revolution, Digital transformation, Artificial intelligence, Penal system, Software complexes, Prevention, Crime

В последнее десятилетие современное общество развивается очень быстрыми темпами. Ряд ученых полагают, что мы стоим у истоков революции (четвертая промышленная революция), которая кардинально изменит нашу жизнедеятельность [1. С. 6]. А может быть, она уже началась? Четвертая промышленная революция характеризуется появлением ключевых технологий (аналитика больших данных, искусственный интеллект, облачные вычисления, моделирование и симуляторы, информационная безопасность), которые все прочнее входят в нашу жизнь. Современное общество в обязательном порядке должно реагировать на происходящие изменения. Все сферы общественной жизни обязаны перестраиваться под новые реалии. Так, 10 октября 2020 г. было утверждено Постановление Правительства Российской Федерации «О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий

в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами» [2], которое установило порядок разработки, утверждения и реализации федеральными органами исполнительной власти ведомственных программ цифровой трансформации.

Уголовно-исполнительная система достаточно оперативно среагировала на складывающуюся в государстве и обществе ситуацию. Спустя два месяца был разработан и утвержден приказ Федеральной службы исполнения наказаний «Об утверждении ведомственной программы цифровой трансформации Федеральной службы исполнения наказаний на 2021 г. и плановый период 2022 и 2023 гг.» [3]. Целями программы закреплены: повышение удовлетворенности граждан государственными цифровыми услугами; уменьшение издержек государственного управления; проведение цифровой трансформации для сокращения теневой экономики и повышения собираемости доходов; повышение надежности и безопасности информационных систем; устранение нагрузки на субъекты предпринимательской деятельности [4. С. 1747]. Поставленные цели планируется реализовывать посредством решения задач по: повышению уровня контроля над безопасностью в исправительных учреждениях; обеспечению полной прозрачности за деятельностью исправительных учреждений; обеспечению бесперебойного функционирования государственных информационных систем уголовно-исполнительной системы; обеспечению всех без исключения учреждений и органов уголовно-исполнительной системы доступом к сети Интернет; выполнению иных государственных функций.

Указанные выше положения и планы нашли свою реализацию во вновь принятой Концепции развития уголовно-исполнительной системы на период до 2030 г [5]. Так, Концепция включает в себя раздел, посвященный цифровой трансформации и научно-техническому развитию уголовно-исполнительной системы. Проведение цифровой трансформации уголовно-исполнительной системы и внедрение цифровых технологий предусматривает:

– создание и внедрение единой информационной системы, обеспечивающей сквозную автоматизацию рабочих процессов;

– применение искусственного интеллекта для создания и развития систем сбора и обработки данных;

– создание единого защищенного управляемого информационного пространства;

– создание методологической и технологической основы для формирования и развития «цифровых» компетенций сотрудников уголовно-исполнительной системы;

– развитие научного потенциала уголовно-исполнительной системы с использованием новых цифровых технологий;

– проведение профильных научных исследований;

– использование видеоконференцсвязи для свиданий осужденных (лиц, заключенных под стражу) с родственниками и контролирующими органами;

– внедрение в деятельность учреждений уголовно-исполнительной системы электронных баз правовой информации.

Реализация указанных выше нормативных актов будет способствовать цифровизации деятельности уголовно-исполнительной системы, ее открытости для общества и повысит общий уровень безопасности [6. С. 69]. Более широкое внедрение цифровых технологий в деятельность уголовно-исполнительной системы должно

способствовать повышению эффективности деятельности по предупреждению пенитенциарных преступлений [7. С. 121]. Указанное выше должно быть реализовано за счет более полного наполнения и оперативного доступа к различным базам данных. В настоящее время в уголовно-исполнительной системе функционирует более 60 различных информационных систем и программных средств. Некоторые из них активно используются в процессе организации предупредительной деятельности путем сбора, хранения и анализа различной информации:

1) программные комплексы автоматизированного картотечного учета спецконтингента являются одними из ключевых систем в деятельности учреждений и органов уголовно-исполнительной системы. Данные комплексы аккумулируют информацию по различным направлениям работы, проводимой с осужденными (подозреваемыми и обвиняемыми) в учреждениях уголовно-исполнительной системы, чем способствуют повышению оперативности формирования и проверки документов;

2) поисковая система подозреваемых, обвиняемых и осужденных «Паноптикум» способствует поиску данных об осужденных (подозреваемых и обвиняемых) в территориально-распределенных базах данных, получению детальной персонифицированной информации;

3) автоматизированная информационная система электронной обработки статистической информации «Статистика УИС» выступает как средство сбора, обработки и анализа статистической информации по различным формам статической отчетности. Данная система позволяет вести центральную базу данных статистической отчетности, а также автоматизировать передачу, прием и обработку статистической отчетности;

4) программное средство «Розыск-контингент» предназначено для повышения уровня информационной обеспеченности подразделений розыска. Программное средство обеспечивает оперативность доступа сотрудников уголовно-исполнительной системы к информации о лицах, находящихся в розыске.

Мы указали лишь некоторые программные комплексы, которые успешно функционируют в деятельности уголовно-исполнительной системы. Реализация политики в области цифровой трансформации будет способствовать повышению эффективности функционирования существующих и созданию новых программных комплексов и систем. Однако в процессе реализации указанных выше планов и концепций не стоит забывать, что излишнее количество информации может отрицательно сказаться на деятельности уголовно-исполнительной системы. Не решив принципиальных вопросов, трудно будет достигнуть целей в частных. Анализ существующей деятельности учреждений и органов уголовно-исполнительной системы показал, что в проводимой цифровой политике существует ряд проблем:

– чрезмерное количество показателей, собираемых и обрабатываемых в отчетной деятельности. Для достижения целей, стоящих перед конкретным программным комплексом, зачастую требуется гораздо меньшее количество уставных данных. Необходимо четко определить тот необходимый минимум, который позволит решить поставленную задачу;

– в деятельности уголовно-исполнительной системе в настоящее время используется более 200 форм статистической отчетности. Одни и те же показатели

собираются с различных исполнителей, что, несомненно, приводит к путанице и искажению данных. Подобная ситуация приводит к ошибкам в финальных подсчетах и мешает оперативной управляемости тем или иным процессом;

– ежегодное увеличение объема информации, требуемой для наполнения программных комплексов, что мешает их нормальному функционированию с учетом несовершенства технических средств;

– неопределенность (а иногда и отсутствие) конкретных, научно-обоснованных критериев оценки деятельности уголовно-исполнительной системы в сфере проходящей цифровизации.

Указанные выше проблемы хорошо прослеживаются при анализе состояния и структуры пенитенциарной преступности, что негативно сказывается на понимании ее реальных показателей и последующем прогнозировании. Представляется, что реализация цифровой трансформации уголовно-исполнительной системы позволит устранить указанные проблемы и повысит эффективность реализуемых предупредительных мероприятий.

Список литературы

1. Шваб К. Четвертая промышленная революция: Эксмо. 2016. 138 с.

2. О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами: Постановление Правительства Российской Федерации от 10.10.2020 № 1646 // Собрание законодательства Российской Федерации. № 42. 19.10.2020 ст. 6612.

3. Об утверждении ведомственной программы цифровой трансформации Федеральной службы исполнения наказаний на 2021 г. и плановый период 2022 и 2023 гг.: Приказ Федеральной службы исполнения наказаний от 30.12.2020 № 984. Документ опубликован не был.

4. Карабанов Р. М., Балакин А. В. Цифровая трансформация уголовно-исполнительной системы // StudNet. 2022. Т. 5. № 3. С. 1746–1754.

5. Об утверждении Концепции развития уголовно-исполнительной системы на период до 2030 г.: Распоряжение Правительства Российской Федерации от 29.04.2021 № 1138-р // Собрание законодательства Российской Федерации. № 20. 17.05.2021 ст. 3397.

6. Черепанова Т. С. К вопросу о цифровой трансформации ФСИН России // В сборнике: Уголовно-исполнительная система сегодня: взаимодействие науки и практики. Материалы XXI Всероссийской научно-практической конференции. Новокузнецк, 2021. С. 69–70.

7. Ковалев С. Д. Цели и стратегические задачи цифровой трансформации уголовно-исполнительной системы // Пенитенциарное право: юридическая теория и правоприменительная практика. 2022. № 1 (31). С. 120–124.

А. А. Петрикина,
кандидат юридических наук, доцент,
Северо-Кавказский филиал
Российского государственного университета правосудия,
Я. С. Примак,
студент,
Северо-Кавказский филиал
Российского государственного университета правосудия

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ: ПЕРСПЕКТИВЫ И ВОЗМОЖНОСТИ

Аннотация. В условиях динамично развивающегося информационного пространства нельзя обойти вниманием исследование возможностей искусственного интеллекта в уголовном процессе нашей страны. Действительно, практически не осталось тех сфер деятельности человека, которые в той или иной степени не затронуты новейшими технологиями: культура, искусство, наука, политика. Юриспруденцию также не обошло вниманием новое веяние. Деятельность следователя, дознавателя, прокурора, судьи по уголовным делам также не является исключением. Целью являлось изучение критериев допустимости использования искусственного интеллекта в производстве по уголовному делу. В настоящей статье проанализированы возможности внедрения искусственного интеллекта в производство следственных и процессуальных действий, перспективы его применения в указанной сфере, затронуты вопросы правовой определенности форм использования искусственного разума в уголовном процессе. Для этого были рассмотрены актуальные научные труды, сделаны выводы о возможной правовой регламентации новейших достижений в действующем уголовно-процессуальном законодательстве Российской Федерации.

Ключевые слова: допустимость, естественный интеллект, искусственный интеллект, суд, судопроизводство, судья, этичность

ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEEDINGS OF THE RUSSIAN FEDERATION: PROSPECTS AND OPPORTUNITIES

Abstract. In the conditions of a dynamically developing information space, it is impossible to ignore the study of the possibilities of artificial intelligence in the criminal process of our country. Indeed, there are practically no areas of human activity that are not affected by the latest technologies to one degree or another: culture, art, science, politics. Jurisprudence has also not been ignored by a new trend. The activities of an investigator, an inquirer, a prosecutor, a criminal judge are also no exception. The aim was to study the criteria for the admissibility of the use of artificial intelligence in criminal proceedings. This article analyzes the possibilities of introducing artificial intelligence into the production of investigative and procedural actions, the prospects for its application in this area, and touches upon the issues of legal certainty of the forms of using artificial intelligence in

criminal proceedings. For this purpose, relevant scientific works were reviewed, conclusions were drawn about the possible legal regulation of the latest achievements in the current criminal procedure legislation of the Russian Federation.

Keywords: Admissibility, Natural intelligence, Artificial intelligence, Court, judicial proceedings, Judge, ethics

В настоящее время существует много различных вариаций значения понятия «искусственный интеллект». Наиболее приемлемым мы считаем следующее: искусственный интеллект – это способность интеллектуальных систем (в число которых входят цифровые компьютеры и роботы, управляемые компьютерами) выполнять те творческие функции, которые традиционно принято считать прерогативой человека. Данный термин часто используется применительно к тем системам, которые наделены такими интеллектуальными процессами, которые свойственны для человека.

Несомненно, искусственный и естественный интеллекты имеют ряд отличий. К примеру, на сегодняшний день ни один созданный искусственный интеллект не достиг такого уровня развития, который бы позволил состязаться «на равных» с человеком [1. С. 708].

В рамках современных научных исследований нередко поднимаются вопросы возможности замены судьи искусственным интеллектом, необходимости подобной замены и процесс внедрения новейших технологий в судопроизводство.

В процессе поиска ответов, хотелось бы отметить, что информационные технологии, а в частности и искусственный интеллект, можно использовать как во благо, так и во вред.

Одной из проблем внедрения искусственного интеллекта в судопроизводство является отсутствие надлежащим образом подготовленных специалистов для разработки программного обеспечения, применяемого в данной сфере. Действующее законодательство закрепляет четкий перечень требований, которые предъявляются к кандидатам на должность судьи. Среди них и соответствующий уровень образования, и определенный жизненный и профессиональный опыт, и высокие моральные качества. А для разработчиков необходимого алгоритма для искусственного интеллекта ничего подобного не требуется. И чаще всего этот алгоритм создается людьми, очень далекими от сферы правосудия.

Также, уголовно-процессуальное законодательство требует от судьи при оценке доказательств руководствоваться более сложными категориями, чем программные алгоритмы. Конечно, современная машина может произвести точный анализ и вынести разумное и верное, с точки зрения закона, решение. Но наряду с формальными признаками, такими, как строгое следование букве закона, в судопроизводстве немаловажное значение имеет и уровень правосознания судьи, его внутренне убеждение в правильности принимаемого решения. И даже элементы правовой психологии, такие как чувства и эмоции судьи, его жизненный опыт являются неотъемлемыми чертами того неповторимого юридического мышления, которое лежит в основе профессии судьи, хоть внешне и осуществляющейся в формальных рамках, но наполненной особым содержанием, неподвластным искусственному интеллекту.

Искусственный интеллект не сможет, в том числе, и проявить гуманность, сострадание и понимание жизненных обстоятельств, причин и условий преступного поведения. Он никогда не научится проникать в мотивы совершенного правонарушения и оценивать правдивость показаний. Машина сможет зафиксировать только факт. Но за каждым фактом скрывается такое понятие как «оценка доказательств» [2. С. 176], внутреннее убеждение судьи, его социальные ценности, профессиональные ориентиры.

Отрицать необходимость использования искусственного интеллекта в различных сферах жизнедеятельности современного государства нельзя, и было бы глупо не воспользоваться его возможностями. Однако уголовный процесс представляет собой ту сферу человеческого бытия, в которой в наибольшей степени уязвимы права и законные интересы личности. В подобной ситуации возникает логичный вопрос, каким образом искусственный интеллект может быть использован в современном судопроизводстве России? В работе А. А. Соколовой в качестве форм использования искусственного интеллекта указаны юридические онлайн-консультации и онлайн-правосудие. Обе эти формы, на наш взгляд, нельзя рассматривать как замену естественного интеллекта искусственным. В первом случае консультацию дают профессиональные юристы, донося информацию до пользователей посредством использования интернет-сервисов. Онлайн-правосудие, по мнению А. А. Соколовой, упрощает взаимодействие граждан с судами и сводится к реализации процедуры подачи документов в электронном виде [3. С. 352]. Это значит, что выполнению чисто технических процедур опять же, посредством использования интернет-сервисов. Ни в одном, ни в другом случае речь не идет о мыслительных процессах.

В современных реалиях перспектива использования искусственного интеллекта в уголовном судопроизводстве видится только одна – исполнение отдельных технических задач.

Рассуждая о внедрении искусственного интеллекта в уголовное судопроизводство необходимо подчеркнуть отсутствие унификации законодательства по данному вопросу и проблемы использования действующих нормативно-правовых актов применительно к расследованию и судебному разбирательству уголовных дел. Многочисленные повторы и пробелы в российском праве не позволяют на сегодняшний день определить границы и критерии использования искусственного интеллекта в уголовном процессе [4. С. 111]. Обсуждение данной проблемы не раз выносилось на всевозможные конференции, велись многочисленные дискуссии, однако лица, участвующие в обсуждении, не могли прийти к общему знаменателю по данному вопросу.

Стоит обратиться к исследованию как положительных, так и отрицательных аспектов использования искусственного интеллекта в уголовном судопроизводстве [5. С. 246].

Среди положительных мы можем выделить следующие: обеспечение расследования и рассмотрения уголовного дела в суде всей необходимой нормативно-правовой базой, которую даже судья, обладающий самой высокой квалификацией, не может знать наизусть; грамотное и продуманное распределение дел между следователями,

дознавателями, судьями при помощи государственных автоматизированных систем с учетом их специализации и нагрузки; дистанционное участие в процессе судопроизводства; снижение уровня нагрузки помощников судей путем делегирования некоторых их полномочий искусственному интеллекту.

Отрицательными же моментами внедрения искусственного интеллекта в уголовное судопроизводство Российской Федерации можно считать следующие: невозможность вынесения решения искусственным интеллектом по аналогии (в тех случаях, когда существует пробел в праве); отсутствие жизненного и профессионального опыта, моральных качеств; невозможность критической оценки в тех или иных ситуациях; недостаточно высокий уровень правового обеспечения.

Рассуждая о методах и способах внедрения искусственного интеллекта в уголовное судопроизводство необходимо акцентировать внимание на том, что данный процесс требует:

– высоких материальных и временных затрат;

– тщательной проработки и определения механизма функционирования, определения направлений использования искусственного интеллекта в уголовном судопроизводстве;

– повлечет за собой значительное уменьшение количества рабочих мест: многие квалифицированные юристы останутся без работы и станут невостребованными на рынке труда, так как с их должностными обязанностями будет справляться алгоритм, заложенный в программу.

Подводя итог вышесказанному, необходимо обратить внимание на то, что УПК РФ требует совершенствования в плане определения в нем форм использования возможностей искусственного интеллекта.

Список литературы

1. Чистилина Д. О. Использование возможностей искусственного интеллекта в уголовном процессе // Вестник Удмуртского университета. Серия «Экономика и право». 2021. № 4. С. 705–710.

2. Бахтеев Д. В. Искусственный интеллект: этико-правовые основы. Москва, Проспект, 2019.

3. Соколова А. А. Искусственный интеллект в юриспруденции: риски внедрения // Юридическая техника. 2019. № 13. С. 350–356.

4. Мосечкин И. Н. Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования. Киров, Вятский государственный университет, 2020.

5. Соколова А. А. Вызовы искусственного интеллекта в юриспруденции: междисциплинарная модель познания // Юридическая техника. 2021. № 15. С. 245–249.

Т. В. Радченко,
кандидат юридических наук,
МИРЭА – Российский технологический университет

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ И УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ОТНОШЕНИЙ

Аннотация. Статья посвящена исследованию искусственного интеллекта на современном этапе развития информационных технологий в России и допустимости его применения на досудебной стадии уголовного процесса. Основная цель заключается в анализе состояния современных информационных систем, использующих искусственный интеллект, возможностях и перспективах их применения в процессе доказывания и оценки доказательств, проведении отдельных следственных действий, составлении процессуальных документов следователем. Подчеркнута необходимость разработки четкого, строгого и эффективного правового режима использования технологии искусственного интеллекта в процессуальной деятельности органов предварительного расследования.

Ключевые слова: цифровизация, искусственный интеллект, правовой режим, защита информации, биометрия, уголовная ответственность, расследование преступлений

THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE SYSTEM OF CRIMINAL LEGAL AND CRIMINAL PROCEDURE RELATIONS НАЗВАНИЕ СТАТЬИ НА АНГЛИЙСКОМ ЯЗЫКЕ

Abstract. The article is devoted to the study of artificial intelligence at the present stage of development of information technologies in Russia. A definition is given on the admissibility of its application at the pre-trial stage of criminal procedure. The main goal is to analyze the state of modern information systems that use artificial intelligence. Showing the possibilities and prospects for the use of artificial intelligence in proving and evaluating evidence, in individual investigative actions, in the preparation of procedural documents by the investigator. It's necessary to develop a clear, strict and effective legal order for the use of artificial intelligence in the procedural activities of the preliminary investigation bodies.

Keywords: Digital transformation, Artificial intelligence, Legal order, Information security, Biometrics, Criminal liability, Crime investigation

Развитие информационных технологий и цифровизация большинства направлений деятельности в современной России стремительно меняет привычный образ экономических отношений и способствует построению системы цифровой экономики как наиболее оптимальной среды применения электронных технологий.

Сегодня цифровизация охватила все сферы и направления общественной жизнедеятельности. Польза цифровизации очевидна. Обладая уникальным инструментарием – искусственным интеллектом, она повышает скорость и эффективность обработки и передачи информации, оптимизируя производственные и технологиче-

ские процессы, уменьшая трудозатраты, и в целом, делая нашу жизнь более удобной. Посредством особых свойств современных компьютерных программ – возможности к обучению, генерации сложных нейронных сетей, способных систематизировать большие объемы данных по заданным параметрам, разрешаются многие сложные задачи.

Нормативная дефиниция искусственного интеллекта как «комплекса технологических решений, позволяющего имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека», закреплена в Национальной стратегии развития искусственного интеллекта на период до 2030 года [1], которая указывает на необходимость «адаптации нормативного регулирования в части, касающейся взаимодействия человека с искусственным интеллектом, и выработки соответствующих этических норм», однако без избыточного регулирования, способного замедлить темп развития и внедрения технологических решений.

Искусственный интеллект – система сложных алгоритмов, которые имитируют когнитивные функции человека. В решении многих задач подобные программы давно перешагнули человеческий интеллект: в части системы распознавания текстов, перевода текстов, распознавания речи. Однако нам не всегда известно, каким образом происходит анализ этих данных, работает ли алгоритм с учетом всех условий и параметров, заложенных разработчиками, насколько исключены ошибки и погрешности при использовании. Будет ли конечный результат объективным.

Глубокие нейронные сети принимают решения не на основе известных алгоритмов, и в ряде случаев проанализировать как они выбирают решение невозможно. Непрозрачность этого алгоритма ведет к тому, что прогноз и проверку результатов осуществить нельзя. И в этом кроется опасность тотального использования искусственного интеллекта, потенциально возрастающая.

Любая компьютерная программа, созданная на основе искусственного интеллекта, сегодня не эффективна даже на 99 %, имеет погрешности, выдает ошибки. Так, современные программы защиты информации эффективны в среднем на 80 % и это отличный результат. Но представим, что искусственный интеллект активно используется в социальной и правоохранительной сферах: для постановки диагноза больному, производит профессиональный отбор сотрудников или квалифицирует преступления. Возможность совершения ошибки при этом колеблется в пределах 20 % случаев, что недопустимо. В каждой из этих ситуаций мы столкнемся с крайне негативными последствиями, влекущими применения мер юридической ответственности.

В связи с вышесказанным актуальным представляется вопрос места искусственного интеллекта в системе правовых отношений и уголовно-процесуальных правоотношений, в частности.

С одной стороны технологии искусственного интеллекта могут выступать в качестве средства оптимизации и повышения эффективности деятельности органов предварительного расследования. Поскольку, реализация уголовно-правовых отношений возможна только в процессуальной форме в соответствии с нормами

УПК РФ представляется возможным в рамках данной работы затронуть сферу уголовно-процессуальных отношений, а именно проведение отдельных следственных действий: допроса и очной ставки, в которых дословная фиксация информации допрашиваемого лица максимально важна. Представляется, что использование искусственного интеллекта при проведении этих следственных действий вполне оправдано и позволит повысить эффективность отображения и сохранения информации при переводе записи голоса в текстовый формат. Это позволит избежать формальных ошибок и неточности изложении при традиционных способах составления протокола следователем.

Фиксацию информации, которая потенциально может иметь доказательственное значение также возможно осуществлять с помощью искусственного интеллекта. Так, использование биометрических систем распознавания лица облегчило работу по пресечению и раскрытию преступлений. Однако в ряде случаев полученные данные требуют всесторонней скрупулезной и качественной проверки на достоверность. В частности, информация, полученная с камер видеонаблюдения, обладающих технологией распознавания лица, не может быть признана прямым и единственно достаточным доказательством, а должна быть проверена и подтверждена иными доказательствами по делу, оцениваемыми в совокупности.

Кроме того, указанная биометрическая информация поступает в хранилища персональных данных и содержит подробные данные о человеке, его внешности, биометрических параметрах, местах нахождения, круге общения, предпочтениях и о многом другом, что позволяет составить характеристику конкретного человека. При этом наблюдается крупномасштабный рост накопления информации в системах устройств прослушивания, анкетирования, тестирования, опросов, видеонаблюдения, в действиях на сайтах. Данные, позволяющие идентифицировать личность, превращаются в товар, который можно продать. Подобная информация может быть использована как в благих целях, например, для ускорения оформления документов, получения услуг, отслеживания преступников, но также с противоправными намерениями: для слежки, компрометации, умаления и дискредитации чести и достоинства, нарушения неприкосновенности частной жизни.

Центром экспертной аналитики InfoWatch был произведен анализ статистики незаконного распространения конфиденциальной информации в последние годы. Так, в 2019 г. было зафиксировано 395 случаев утечек данных из российских фирм и государственных учреждений. Объем кажется небольшим в масштабах страны, но, если возможно получить даже такую малую часть, значит, есть потенциальная возможность украсть и другие данные. [2] В последующие годы количество подобных инцидентов продолжало возрастать. Современные масштабы сбора и использования персональных данных хорошо иллюстрирует цитата Эрика Шмидта, возглавляющего Alphabet: «Постепенно вы, как реальный человек, будете интересовать мир все меньше и меньше, а значение вашего цифрового аватара, наоборот, станет неуклонно повышаться, поскольку он очень многое о вас может сказать. Всех будет интересовать ваша цифровая копия, которая хранится в облаках, а не вы. При этом важно понимать, что все

мы будем абсолютно прозрачны для цифрового мира… это ключевой тренд на ближайшие годы» [3].

Сегодня остро стоит проблема создания эффективного и детализированного правового режима, регулирующего использование технологии распознавания лиц как одного из направлений биометрии. Она внедряется практически повсеместно, и активно используется правоохранительными органами при раскрытии и расследовании преступлений в качестве доказательства.

Однако на сегодня не существует систем защиты биометрической информации. Пока их нет, использование этой информации в целях доказывания требует осторожности и тщательной проверки, поскольку в отличие от логинных систем, где информацию можно поменять, в биометрической системе это абсолютно невозможно. Поскольку биометрическая информация на порядок чувствительнее любой другой, то и системы защиты должны быть на порядок выше: даже 1 % ошибок в их работе – это катастрофа, когда чужое лицо распознается как ваше или ваше лицо не распознается. Обе эти ошибки существуют и до сих пор, эффективность работы биометрических систем измеряется процентами, а для по-настоящему эффективной работы, по мнению специалистов должна измеряться 10-тысячными долями процента.

Стремительное развитие информационного общества привело к отставанию в детальном правовом обеспечении данной сферы. При формировании правовых норм, направленных на регулирование применения технологии распознавания лиц, а также использование персональных данных, важное значение имеет определение закономерностей и перспектив развития, анализ законодательной стратегии и тактика правоприменительной практики в этой сфере. Исследуемая проблема требует нового концептуального подхода, исходя из возникающих угроз и в связи с трудностями определения правовой природы указанных информационных феноменов.

Представляется, что сегодня использование искусственного интеллекта затруднительно при осуществлении аналитических мероприятий, требующих высокой степени анализа и оценки всех обстоятельств совершенного деяния. Речь идет о процессе уголовно-правовой квалификации, которая невозможна, на наш взгляд, только с помощью искусственного интеллекта. Каждое преступление помимо признаков элементов состава обладает также и особыми индивидуальными свойствами, учитывать которые должен и искусственный интеллект. Слишком высока в этом процессе роль правоприменителя, его аналитические способности, умение систематизировать и структурировать информацию и на основании этого соотносить обстоятельства совершенного деяния, признакам элементов состава преступления. Очевидно, что каждое противоправное, преступное деяние обладает индивидуальными свойствами, при этом ни одна программа, использующая свойства искусственного интеллекта, не обладает такой широкой вариативностью как человеческий разум. Кроме того, точность и правильность результатов квалификации, осуществляемой искусственным интеллектом, потребует от пользователя внесения исходных данных, а это только затруднит работу следователя/дознавателя, сделает ее наоборот более рутинной.

Подводя итог сказанному, следует отметить, что проблема нормативного закрепления правовой регламентации использования искусственного интеллекта при осуществлении процессуальных действий при осуществлении предварительного расследования требует незамедлительного решения. Основной целью при этом должна стать не попытка заменить человеческий разум компьютерной программой, использующей искусственный интеллект, а оказание помощи правоприменителю в проведении отдельных следственных и процессуальных действий, фиксации материалов расследования в целях оптимизации и повышения эффективности деятельности.

Список литературы

1. Указ Президента Российской Федерации от 10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». URL: http:// Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.10.2019, «Собрание законодательства РФ», 14.10.2019, № 41, ст. 5700 (дата обращения: 19.02.2022).

2. Утечки данных. Россия. 2019 год. Аналитический центр Infowatch. URL: https://www.infowatch.ru/analytics/reports/27614 (дата обращения: 19.02.2022).

3. Четверикова О. Цифровой тоталитаризм. Как это делается в России? – М.: Книжный мир. 2019 // URL: https://iknigi.net/avtor-olga-chetverikova/183838-cifrovoy-totalitarizm-kak-eto-delaetsya-v-rossii-olga-chetverikova/read/ (дата обращения: 19.02.2022).

В. В. Ровнейко,
кандидат юридических наук, доцент,
Удмуртский государственный университет

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ «КРАЖИ ИДЕНТИФИКАЦИИ»

Аннотация. Статья посвящена анализу такого понятия как «кража идентификации» и проблемам уголовно-правовой оценки деяний, которые посягают на безопасность цифровой личности. Введение экспериментальных правовых режимов, реализация «пилотных проектов» в «регуляторных песочницах» выявляют новые виды рисков, которые должны быть минимизированы. Так, один из проектов, связанный с использованием биометрических персональных данных при предоставлении банковских услуг, был запущен как регулятивная «песочница» Банка России. Однако «пилот» не взлетел из-за серьезных рисков подделки биометрических данных и документов. Неправомерное использование чужих персональных данных для получения выгоды является «кражей идентификации». Определение понятия «кража идентификации» с учетом положений российского законодательства нуждается в существенной коррекции. Уголовно-правовые средства позволяют рассматривать в качестве основания уголовной ответственности за «кражу идентификации» составы различных преступлений, предусмотренных в УК РФ (например,

о мошенничестве), но необходима разработка системы мер, как уголовно-правового, так и регулятивного характера для обеспечения безопасности цифровой личности.

Ключевые слова: уголовное право, цифровые технологии, «кража идентификации», цифровая личность, безопасность цифровой личности, «регуляторные песочницы», экспериментальный правовой режим

CRIMINAL LAW PROBLEMS OF «IDENTITY THEFT»

Abstract. The article is devoted to the "identity theft" and to the problems of criminal law assessment of acts that infringe on the security of a digital identity. The introduction of experimental legal regimes, the implementation of "pilot projects" in "regulatory sandboxes" reveal new types of risks that should be minimized. As a regulatory sandbox of the Bank of Russia one of the projects using biometric personal was related in the provision of banking services. There are serious risks of forgery of biometric and documents in the "pilot". The misuse of other people's personal for profit is "identity theft". The definition of "identity theft", taking into account the provisions of Russian legislation, needs significant correction. In Criminal law there are corpus delicti to criminal liability for "identity theft". The corpus delicti of various crimes provided in the Criminal Code of the Russian Federation (for example, fraud) can be use for "identity theft", but it is necessary to develop a system of measures, criminal and regulatory in nature to ensure the security of a digital identity.

Keywords: Criminal law, Digital technologies, "Identity theft", Digital identity, digital identity security, "Regulatory sandboxes", Experimental legal regime

Применение в различных сферах деятельности цифровых технологий порождают возникновение социально значимых ценностей (общественных отношений, интересов и благ), находящихся за пределами охраны действующего уголовного законодательства России. Принятие Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [17] и введение «пилотных проектов», «регуляторных (цифровых) песочниц» [6] в различных сферах деятельности породили большое количество вопросов организационного, технического, морального и правового, в том числе и уголовно-правового характера.

Один из таких проектов связан с использованием биометрических персональных данных [12] при предоставлении банковских услуг и запущен как регулятивная «песочница» Банка России (т. е. «механизм для пилотирования, моделирования процессов новых финансовых сервисов и технологий в изолированной среде, требующих изменения правового регулирования») [13]. Восемнадцать российских банков приняли участие в проекте для тестирования возможности открытия счетов новым клиента с применением видеоконференцсвязи без посещения отделения банка физическим лицом. Национальным советом финансового рынка (НСФР) была направлена заявка в Банк России (ЦБ) на пилотирование указанной технологии в регулятивной «песочнице» ЦБ. Данный проект нуждается в тщательном изучении пилотировании в «песочнице» Банка России, так как идентификация лица по

видеосвязи связана с высокими рисками для граждан и финансовых организаций» [19]. «Пилот» не взлетел в связи с серьезными рисками подделки биометрических данных (видео и голоса), а также документов. Работа над проектом продолжается, и банки ищут способы минимизации рисков мошенничества [3].

Хотя указанный проект не был завершен и Банк России не инициировал процедуру создания правовых условий для внедрения сервиса [13], попытка реализации проекта выявила серьезную проблему, связанную с возможной «кражей идентификации» [16] («кражей личности» [2], «кражей идентичности» [10], «похищения цифровой личности» [2] и т. п.) и неправомерным использованием чужих персональных идентификационных данных в своих интересах. Закрепленный в ст. 2 Конституции РФ приоритет интересов личности и возникновение «цифровой личности» обуславливают необходимость обеспечения цифровой безопасности личности уголовно-правовыми средствами и делают необходимым изучение возможностей действующего уголовного законодательства России в этой сфере.

Возникновение новых социально значимых ценностей, в том числе, таких как «цифровая личность», обусловленных применением в различных сферах деятельности цифровых технологий, может повлечь возникновение пробела в уголовном законе. Такой пробел не может восполняться путем применения уголовно-правовых норм по аналогии. В результате некоторые объективно общественно опасные деяния не подпадают под действие уголовно-правовых норм. Нельзя сказать, что все посягательства на такие ценности полностью находятся за пределами действия Уголовного кодекса РФ.

Если рассмотреть риски, которые возникают при удаленной идентификации личности для получения банковских услуг, в уголовно-правовом аспекте, то можно сделать вывод о том, что многие из них формально содержат признаки составов преступлений, предусмотренных в УК РФ. Так, в ходе рассмотрения и анализа возможности применения данного сервиса ЦБ, Минфин и Росфинмониторинг определили пять видов рисков [20].

Необходимо отметить, что большинство из перечисленных в качестве рисков деяний представляет повышенную опасность в связи с техническими сложностями идентификации лица, использующего чужие персональные идентификационные данные. Большая часть из них может быть квалифицирована как мошенничество с учетом разъяснений, содержащихся в постановлении Пленума Верховного Суда РФ о видах и содержании обмана [7], или как отмывание доходов от преступной деятельности [8]. Особая опасность таких действий связана, прежде всего, с возможностью причинения имущественного ущерба как кредитным организациям, так и их клиентам при реализации сервиса по удаленному предоставлению банковских услуг с использованием для идентификации клиентов персональных биометрических данных, лицами, установить которых для последующего привлечения к уголовной ответственности достаточно сложно.

Повышенный интерес с точки зрения уголовно-правовой оценки содеянного представляют подмена изображения и подмена личности клиента, которые могут рассматриваться как особый способ совершения преступления. Для обозначения этих общественно опасных действий используется понятие «Identity theft» или «кража

идентификации», под которой понимается причинение вреда путем неправомерного использования персональных данных другого лица. Хотя неправомерному использованию могут подвергнуться данные как физического, так и юридического лица, мы будем рассматривать содержание данного понятия в отношении только физических лиц.

Следует отметить, что характер общественной опасности при «краже идентификации» (Identity theft) не сводится только к причинению имущественного ущерба, хотя в большинстве источников в качестве признака данного вида преступления указана направленность деяния на «получение материальной выгоды» [11]. В других источниках содержится более широкое понятие, в котором в качестве признака «кражи личности (identity theft)» указана направленность на получение любой выгоды [2]. В условиях отсутствия нормативного определения оба подхода имеют равное значение. Но ограничивать количество случаев «кражи идентификации» только корыстной направленностью было бы нецелесообразно.

IT-специалисты выделяют виды «кражи личности» в зависимости от целей последующего использования полученной идентификационной персональной информации. В одной из таких классификаций, например, выделяют в качестве видов кражи личности: 1) финансовые махинации; 2) преступная кража личности (identity theft); 3) кража данных с целью изменения личности; 4) похищение медицинских данных; 5) создание клонов[2].

Данная классификация представляется не вполне корректной, так как ее авторы рассматривают «кражу личности» и как отдельное явление, и как его разновидность (такая кража-кража личности).

В другой классификации авторы тоже выделяют пять видов «кражи идентификации», но немного иначе: 1) кража личных данных; 2) кража финансовой идентичности; 3) кража детской личности; 4) кража личных данных налогоплательщика; 5) кража медицинской идентичности [21].

Таким образом, авторы второй классификации, рассматривая как самостоятельные виды кражу личных данных ребенка и кражу личных данных налогоплательщика, не выделяют в качестве самостоятельного вида создание клонов и кражу личных данных для изменения личности. Представляется, что похищение биометрических персональных данных, которые могут быть использованы для «создания клонов» и «изменения личности», необходимо рассматривать в качестве самостоятельного вида «кражи личности» и с учетом технических особенностей таких действий, а также существование рисков подделки биометрических данных (видео и голоса), например, для дистанционного получения банковских услуг.

Вышеприведенные классификации составлены не юристами, а специалистами в области IT. Имеющиеся правовые исследования в этой сфере не содержат исчерпывающей классификации «краж идентификации», хотя и посвящены правовым проблемам противодействия этому явлению (их немного) [1, 4, 14, 15]. Доктринальные правовые определения понятия «кража идентификации» разнообразны. Одни авторы рассматривают это понятие только в очень узком смысле и приравнивают его к мошенничеству [15]. Другие используют вместо понятия «identity theft» в качестве синонима понятие «digital identity theft» (кража цифровых идентификационных данных), определяя его «доступ к персональной информации

лица, его документам (точнее, их цифровым копиям), данным банковских карт и так далее, в результате чего возникает возможность совершить хищение имущества, принадлежащего такому лицу, либо продать полученные доступы третьим лицам» [1]. Третьи определяют identity theft как кражу личности, и сделку, заключенную, как правило, неустановленным лицом под чужой личиной путем подлога документов и подделки подписей, будь то бумажных или электронных» [14]. Из вышеприведенных точек зрения наиболее обоснованным представляется подход, когда «кража идентификации» рассматривается как «кража цифровых идентификационных данных». Последняя отражает суть анализируемой уголовно-правовой проблемы наиболее точно.

Понятие «кража личности» тесно связано с понятием «цифровой личности». Нормативного определения указанного понятия нет. Давая доктринальное определение в юридической литературе цифровую личность определяют «как совокупность данных о субъекте, отраженная в цифровой форме и содержащая достоверную информацию, включая (но не ограничиваясь) персональные данные субъекта – физического лица или сотрудников юридического лица, финансовую, правовую и банковскую информацию, сведения о его интересах и предпочтениях, историю покупок и перемещений, а также иные сведения, позволяющие осуществить идентификацию субъекта – правообладателя информации или иного лица, связанного с такой информацией» [1].

Понятие «цифровой личности» может быть в некоторых случаях отождествлено понятию «цифровой профиль», под которым может пониматься «совокупность сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в единой системе идентификации и аутентификации»» [9]. Полагаем, что с учетом такого определения «цифровой профиль» является более узким понятием по сравнению с «цифровой личностью».

«Кража идентификации» («кража цифровой личности») не ограничивается только корыстной направленностью и, по нашему мнению, должна рассматриваться в широком смысле этого понятия, хотя следует согласиться с тем, что в подавляющем большинстве случаев она совершается в целях получения прямо или косвенно материальной выгоды, но при этом не всегда причиняет вред имущественным правам потерпевшего, хотя всегда нарушает личные права и законные интересы физического лица, чьи персональные данные были похищены. В существующих определениях понятия «identity theft» особое значение придается получению выгоды, а использование неправомерного доступа к цифровому объекту является вторичным. Следует согласиться с мнением, что буквальный перевод на русский язык понятия «identity theft» как «кража идентификации» или «кража цифровой личности» – «представляется не вполне корректным, поскольку фактически происходит завладение не цифровым объектом, а, скорее, доступом к нему» [1].

Необходимо отметить, что уголовно-правовые нормы не предусматривают уголовную ответственность за сам факт «кражи идентификации», т. е. незаконного получения (собирания) или подделки (изготовления) персональных цифровых

идентификационных данных личности. Регулятивное законодательство определяет правовой режим персональных данных. Право на получение персональные данные с последующим внесением их в Единую биометрическую систему имеют самые разные субъекты (и банки, в том числе). В таких условиях, когда получать и собирать информацию могут разные субъекты, и возникает проблема ответственности за их утечку или другие неправомерные действия с такой информацией.

В Российской Федерации формируется Единая биометрическая система (ЕБС), инициаторами создания которой являются банки и ЦБ, а исполнителем – «Ростелеком». Данные, содержащиеся в ЕБС, востребованы в различных сферах жизни, например, в сферах здравоохранения, образования, ритейла, государственных услуг. Наиболее широкое применение ЭБС имеет в финансовой сфере в коммерческих банках [5].

С учетом действующего механизма удаленной идентификации и этапов удаленной идентификации [5], в котором задействованы как вышеуказанные государственные органы, так и физические лица, можно утверждать, что подмена персональных данных может иметь место и при совершении регистрации физического лица в ЕСИА или ЭБС, так и совершении физическим лицом действий по удаленной регистрации.

В отношении идентификационных персональных данных необходимо предусмотреть самостоятельный механизм уголовно-правовой защиты, исходя из того, что «персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)», и с учетом различного вида таких данных (по содержанию, по особенностям правового режима, по источнику и т. п.) [18]. Но, поскольку законно получать и собирать информацию о личности могут разные субъекты, то необходима и дифференциация уголовной ответственности в зависимости от формы вины, целей и мотивов, а также тяжести наступивших последствий (количества потерпевших, характера и размера причиненного им вреда). Кроме того, необходимо учитывать, что многие понятия, которые используются при описании посягательств на информационную безопасность, включая информационную (цифровую) безопасность личности, носят технический характер.

Как известно, корректность и единообразие используемых формулировок позволяет решить многие правовые проблемы. Имеющиеся расхождения в понятиях, имеющих одинаковое (или почти одинаковое содержание), должны учитываться при определении криминообразующих признаков. В сфере информационных технологий общепринятым является использование английских терминов, которые будучи дословно переведенными на русский язык, не могут быть использованы в качестве юридических формулировок сами по себе. Установление уголовной ответственности за «кражу идентификации» предполагает тщательный выбор терминологии и корректное использование специальных технических понятий.

Для корректного использования в понятии «кража идентификации» термина «идентификация» следует учитывать, что и она имеет определенное содержание. И с учетом этого содержания нельзя отождествлять идентификацию с другими схожими терминами. Так, в специальной литературе отмечается, что «часто в рос-

сийской практике термином «идентификация» называют три понятия, а именно: собственно идентификацию, верификацию и аутентификацию [5], которые имею близкое по характеру, но все-таки различное содержание, которое необходимо учитывать для понимания правовой природы такого явления как «identity theft». Под идентификацией в узком смысле понимается установление совпадения неизвестного объекта известному; под аутентификацией понимается удостоверение личности; а под верификацией – подтверждение подлинности документов [5].

Таким образом, установление уголовной ответственности за незаконные получение и использование или сбыт персональных данных физического лица, которые позволяют осуществить идентификацию, верификацию и аутентификацию личности является необходимым, исходя из развития инновационных цифровых технологий в различных сферах деятельности.

Некоторые авторы не считают «цифровую личность» новым правовым явлением, нуждающимся самостоятельной правовой охране. Они выделяют два основных аспекта «цифровой личности»:

– «цифровые копии документов, содержащих персональные данные субъекта, его медицинские данные и прочие индивидуальные характеристики, закрепленные в цифровой форме,

– информация о его сетевой активности, история запросов в браузере, предпочтения, интересы и иная информация, которая носит менее формальный характер, нежели первая категория, но также представляет собой высокую ценность, как с точки зрения правомерного коммерческого использования, так и для потенциальных правонарушителей» [1].

С учетом этого подхода и «понимания цифровой личности как цифровой фиксации идентифицирующих документов и прочей информации, содержащей персональные данные о субъекте», ими предлагается «вывод о том, что должен применяться режим, аналогичный бумажным документам,» [1] и «режим конкретных составляющих цифровой личности должен соответствовать потенциальным целям существования информации в той или иной форме: применительно к документам (например, паспорт, ИНН, трудовая книжка, медицинская карта и т. д.)», должен применяться «режим, аналогичный документам в их материальном выражении» [1]. В отношении второй группы информации – персональных данных – должен применяться режим, установленный российским законодательством, согласно которому история поиска и прочая информация, полученная без ведома гражданина, может быть предложена к обработке в рамках режима персональных данных либо коммерческой тайны (в случае обезличенной обработки и использования, например, в рамках формирования статистики)» [1].

Применение к электронным документам (цифровым документам) правового режима, аналогичного применяемому к бумажным документам, общепризнано [22]. Но персональная информация, которая не носит такого формально-документированного характера (например, видео-идентификация) не охраняется нормами уголовного права, если не является личной или семейной тайной [23].

Необходимо отметить, что предлагаемые подходы, применим в области гражданского права, одним из принципов которого является добросовестность и разумность

поведения участников общественных отношений. Задачей уголовного права является охрана прав и свобод личности от общественно опасных действий (бездействия). «Цифровая личность» (digital identity) и цифровые права нуждаются в самостоятельной уголовно-правовой охране, но это возможно только после определения регулятивным законодательством содержания персональных данных («цифровой личности») и режима получения (сбора), хранения, передачи, предоставления, использования и уничтожения персональных данных, позволяющих осуществлять идентификацию, верификацию и аутентификацию личности. Только в этом случае могут быть определены криминообразующие признаки для установления уголовной ответственности за неправомерное использование (а также получение, хранения и т. д.) персональных данных и за нарушение правил использования (а также получения, хранения и т. д.), повлекших их утечку.

Необходимость такого самостоятельного правового регулирования этой сферы деятельности признается даже теми авторами, которые пришли к выводу, что «цифровая личность не представляет собой качественно новое явление, а является новым способом закрепления существующей информации» [1]. По их мнению, все-таки «требуется внесение соответствующих изменений в существующее законодательство для отражения правового режима персонализированной информации посредством цифровой формы. Кроме того, сама категория цифровой личности подлежит детальному рассмотрению в рамках научной и учебной деятельности» [1].

Таким образом, выявленные риски «применения систем видеосвязи или иных технических средств для удаленной идентификации клиентов банков в «регуляторной песочнице» ЦБ» были реальными, «поэтому пилот не взлетел» [20]. Такие риски не могут быть минимизированы или устранены путем применения только уголовно-правовых мер. Предпринимаемые меры должны носить комплексный и системный характер. Но выстраивание комплаэнса, направленного на обеспечение цифровой безопасности личности (безопасности цифровой личности) невозможно без использования уголовно-правовых средств противодействия. Закрепление в уголовном законе признаков состава преступления (или составов преступления), которые могут рассматриваться как «кража идентификации», в таких условиях становится необходимой.

Использование цифровых технологий в отношении идентификации, верификации и аутентификации личности при отсутствии средств и гарантий должной защиты личности от неправомерного использования ее биометрических данных является необоснованным риском применения технологий и сервисов, предполагающих сбор и использование того, что может рассматриваться как «цифровая идентификация». Такое использование нуждается в серьезном, глубоком и разностороннем изучении, как с позиций разработки условий правомерности причинения вреда в состоянии обоснованного риска, так и таких понятий, как «цифровая личность», «цифровой профиль» и цифровые права.

«Кража идентификации» предполагает неправомерное получение данных о субъекте, отраженных в цифровой форме, включая персональные данные, которые позволяют осуществить идентификацию (идентификацию, верификацию и аутентификацию) субъекта. Дальнейшее использование такой информации может осуществляться

в самых разных целях и «кражей идентификации» с учетом понятийного аппарата, используемого уголовным правом России, не является. Более корректным было бы в этом случае говорить о «похищении цифровых идентификационных данных».

С учетом действующего российского уголовного законодательства случаи незаконного использования персональных данных можно рассматривать как способы совершения преступлений, уже содержащихся в УК РФ и совершаемых, как правило, путем обмана (мошенничества, умышленного причинения имущественного ущерба при отсутствии признаков хищения и др.). Но представляется возможной дифференциация уголовной ответственности с учетом повышенной общественной опасности таких деяний, совершаемых с использованием незаконно полученных или незаконно используемых цифровых идентификационных данных

В случае установления правового режима «цифровой личности» корректной будет и постановка вопроса об уголовно-правовом значении как предмета самостоятельного состава преступления элементов «цифровой личности» – персональных данных, биометрических персональных данных, медицинских данных, данных налогоплательщика и информация о сетевой активности, история запросов в браузере, предпочтения, интересы и иная личная информация.

Список литературы

1. Кирсанова Е. Е. Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике: монография. М.: Юстицинформ, 2022. 228 с. / СПС «КонсультантПлюс».

2. Кража личности (Identity theft) // URL: https://www.anti-malware.ru/threats/identity-theft (дата обращения: 19.08.2022).

3. Лекомцева Н. Что такое «регуляторная песочница». Объясняем простыми словами //Энциклопедия. 24 сентября 2021 год. URL: https://secretmag.ru/enciklopediya/chto-takoe-regulyatornaya-pesochnica-obyasnyaem-prostymi-slovami.htm (дата обращения: 19.08.2022).

4. Минаева А. И. Цифровые права как элементы правового статуса личности // Вопросы российского и международного права. 2021. Том 11. № 3А. С. 69–77. DOI: 10.34670/AR.2021.81.43.035 URL: https://www.elibrary.ru/download/elibrary_46126392_10550362.pdf (дата обращения: 19.08.2022).

5. Метревели Е. Г. Перспективы развития цифровой идентификации личности // Современная наука: актуальные проблемы теории и практики. Серия «Экономика и право». № 12, декабрь 2021. С. 71. URL: http://www.nauteh-journal.ru/files/dc428735–3a20–4622-b9dc-4ccf948dda4b (дата обращения: 19.08.2022).

6. Постановление Правительства РФ от 9 марта 2022 г. № 309 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств». URL: https://base.garant.ru/403712648/ (дата обращения: 17.09.2022).

7. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 17.09.2022).

8. Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» URL: http://www.consultant.ru/document/cons_doc_LAW_182365/ (дата обращения: 17.09.2022).

9. Проект федерального закона № 747513–7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» (ред., внесенная в ГД ФС РФ, текст по состоянию на 05.07.2019) // СПС «КонсультантПлюс» (дата обращения: 17.09.2022).

10. Подлог, связанный с применением компьютеров. URL: https://studref.com/693043/pravo/podlog_svyazannyy_primeneniem_kompyuterov

11. Переход на личности: что такое identity theft. URL: https://www.securitylab.ru/blog/company/infowatch/341488.php (дата обращения: 19.08.2022).

12. Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) о вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки. URL: https://25.rkn.gov.ru/news/news54167.htm (дата обращения: 17.09.2022).

13. Регулятивная «песочница» Банка России. URL: https://cbr.ru/fintech/regulatory_sandbox/ (дата обращения: 19.08.2022).

14. Рудоквас А. Д. О влиянии регистрационной системы на оборот недвижимости // Вестник гражданского права. 2022. № 1. С. 45–58. / СПС «КонсультантПлюс» (система).

15. Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» (2-е издание, переработанное и дополненное). («Статут», 2021) / СПС «КонсультантПлюс».

16. Сазонова Маргарита. Биометрические персональные данные и технологии идентификации: какие правовые проблемы могут возникнуть? // URL: https://www.garant.ru/news/1460152/ (дата обращения: 19.08.2022).

17. Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» от 31.07.2020 № 258-ФЗ (в ред. Федерального закона от 02.07.2021 № 331-ФЗ) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_358738/ (дата обращения: 17.09.2022).

18. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» п. 1 ст. 3 / СПС «Консультант».

19. Чернышова Евгения. «Банки протестируют открытие счетов клиентам по видеосвязи. Но пока ограничат объем операций, которые можно проводить таким способом» // РБК. 09.11.2020. URL: https://www.rbc.ru/finances/09/11/2020/5fa3f7769a79477c927c9189 (дата обращения: 19.08.2022).

20. Чернышова Евгения. ЦБ увидел угрозу при идентификации банковских клиентов по видео. Среди рисков – использование дипфейков и профессионального грима // Финансы, 21 мая 2021 – РБК. URL: https://www.rbc.ru/finances/21/05/2021/60a664d49a79472499fee709 (дата обращения: 19.08.2022).

21. Что такое кража личных данных? URL: https://ru.gofreedommoney.com/what-is-identity-theft (дата обращения: 19.08.2022).

22. Пленум Верховного Суда Российской Федерации принял новое постановление № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных статьями 324–327.1 УК РФ» URL: https://www.vsrf.ru/documents/own/29494/ (дата обращения: 19.08.2022).

23. Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» URL: http://www.consultant.ru/document/cons_doc_LAW_314616/ (дата обращения: 19.08.2022).

Г. В. Романова
кандидат юридических наук,
Казанский институт (филиал) Всероссийского государственного
университета юстиции

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация. В современном мире неизбежно возрастает роль цифровых возможностей и цифровизации услуг в различных сферах жизнедеятельности. В уголовном судопроизводстве появляется и развивается такой вид (источник) доказательства как электронное доказательство. В настоящей статье представлены актуальные вопросы использования электронных доказательств в уголовном судопроизводстве.

Ключевые слова: уголовный процесс, компьютерная информация, электронное доказательство, цифровое доказательство

PROBLEMS OF USING ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Abstract. Digitalization of criminal procedural activity is a complex process that inevitably affects the procedure of proof. One of the most controversial topics in this direction remains the possibility of introducing a new type (source) of evidence – electronic evidence. The article deals with topical issues in criminal proceedings.

Keywords: Criminal proceedings, Computer information, Electronic evidence, Digital evidence

Вопросы доказательств и доказывания приобретают процессуальное значение и активно исследуются учеными и правоприменителями в уголовном судопроизводстве.

Представляется, что изучение специального предназначения электронных доказательств в уголовном процессе связана с двумя методологическими проблемами. Во-первых, электронному доказательству придается первостепенное значение, изучается техническая сторона вопроса. Во-вторых, понимание электронного доказательства связано с электронной структурой документа, что затрагивает его особые свойства носителя.

Проблематика также содержится и в том, что электронные доказательства не всегда могут быть самостоятельным источником доказывания. Уголовно-процессуальное законодательство не разграничивает электронные доказательства на группы, что затрудняет их поиск и применение в практической деятельности юриста.

Одновременно вопрос о возможной классификации электронных доказательств представляет доктринальный интерес. Электронные доказательства очень часто подразделяются на те, доступ к которым свободен и тех, которые находятся в ограниченном поле доступа.

Среди электронных доказательств, находящихся в общем доступе, выделяется информация, ставшая известной из интернет-сайтов, сервисов социальной сети, например, «ВКонтакте», «Одноклассники», «Твитер», Facebook (Facebook, Twitter – признанные экстремистскими социальные сети, запрещенные в Российской Федерации), Linkedln и других. А также активно используемых пользователями новостных страничек средств массовой информации государственного и частного формата.

В следственной и судебной практике очень часто используются сведения, взятые из открытых интернет-источников, проверенные и оформленные надлежащим образом с учетом всех требований уголовно-процессуального закона.

В качестве примера обратим внимание на особенности расследования уголовного дела о публичных призывах к осуществлению террористической деятельности, поддержке терроризма с использованием информационно-телекоммуникационной сети Интернет. В ходе расследования органами предварительного расследования были составлены протоколы:

– об изъятии информации, содержащейся на страничке социальной сети «ВКонтакте», с копией текстовых сообщений и фотографиями, призывающими к совершению террористического акта;

– осмотра документов, подтверждающих связь абонентского номера с идентификационной страничной в социальной сети «ВКонтакте», с помощью которой распространялся компрометирующий материал.

Кроме того, по судебным решениям органами предварительного расследования были установлены адреса электронных почт, серверов, провайдеров, используемых для подключения абонента к социальной сети «ВКонтакте».

Правоохранительные органы установили постоянное место с указанием точного адреса квартиры подозреваемого с подключением к социальной сети и транслированием запрещенных фото и видеоматериалов, поддерживающих и оправдывающих терроризм.

На начальном этапе расследования была исключена возможность взлома личной странички в социальной сети подозреваемого, в связи с чем были предоставлены материалы, которые опровергали обращение в службу безопасности «ВКонтакте» подозреваемого.

Осмотр личной странички в социальной сети подозреваемого проводился в присутствии незаинтересованных лиц, о чем свидетельствовала отметка в протоколе.

Свидетели сообщили суду о том, что осмотр личной страницы подсудимого в социальной сети «ВКонтакте» осуществлялся в режиме реального времени [2].

Приговором суда ему было назначено наказание за публичный призыв к осуществлению террористической деятельности с учетом части 2 статьи 205.2 УК РФ. Апелляционным судом ранее вынесенный приговор с учетом наказания виновного был оставлен без изменения.

Вопрос о возможности использования информации, полученной из средств массовой информации и информационно-коммуникационной сети «Интернет», был предметом исследования Пленума Верховного Суда России, который в своем решении [3] обратил внимание правоприменителя о том, что если публичный призыв к осуществлению террористической деятельности или оправдание терроризма происходят с использованием интернет-сайтов, то содеянное подлежит квалификации по части 2 статьи 205.2 УК РФ.

Особый интерес получения доказательств в электронном виде получает свое развитие в результате совершенствования методов, способов, технических средств и устройств, способных не только раскрыть совершенное преступление, но и указать на подготовку к нему. В этой связи обращают на себя такие технические средства, как фитнес-браслет, кардиостимулятор. В зарубежных странах информация, полученная путем сканирования указанных устройств, весьма успешно используется правоохранительными органами для подтверждения события преступного действия. Но в российской следственной и судебной практике такие данные в качестве доказательств не используются. В большинстве случаев ходатайства об исследовании фитнес-браслетов, которые способны содержать информацию о непричастности к причинению тяжких телесных повреждений и приобщения их в качестве доказательств к материалам дела судебными и следственными органами остаются без рассмотрения [4].

Иной проблемой электронного доказательства становится его отрыв от реальности и поглощение виртуальным характером его восприятия. «Реальный» и «виртуальный» мир активного повседневного пользователя интернет-ресурса отличается. «Виртуальное» интернет-пространство эффектно адаптируется к различным реалиям и пожеланиям своего интернет-пользователя, угадывая и подстраиваясь под возможности и желания своего пользователя. Юридическую оценку искусственный интеллект получает в случае необходимости установления всех участников правоотношений, пользователей информационно-коммуникационной сети Интернет в определенный день, час, месяц, год.

С уголовно-правовой позиции свободное интернет-пространство обладает огромными последствиями. С помощью него можно подтвердить, или наоборот, опровергнуть, юридически важные события, создать дополнительные процессуальные гарантии участникам уголовного судопроизводства.

В качестве примера приведем следующий случай из практики. Использование репостов в социальных сетях не является новым продуктом для граждан нашей страны. Такая нейтральная по своей природе форма активности пользователей в интернет-пространстве, позволяет делиться информацией, своими мыслями, мнением. Однако распространяемые сведения не всегда носят правдивый характер, что создают угрозу распространения ложных, непроверенных слухов. Пленум Верховного Суда России обратил на это свое внимание [5]. Он указал, что распространение репостов, содержащих ложную информацию, может квалифицироваться

по статьям 207.1 и 207.2 УК РФ, но только в том случае, когда будет установлено, что лицо, выложившее такую информацию, действовало с прямым умыслом и сознавало, что размещенные им сведения под видом достоверных являются неправдивыми. При этом цель злоумышленника вполне логична, он хочет довести ложную информацию для других лиц, действуя при этом осознанно.

В заключение отметим, что проблемы использования электронных доказательств в уголовном судопроизводстве имеются, но они решаемы. На сегодняшний день цифровое пространство получило повышенное внимание в работе органов предварительного расследования и суда. Виртуальное пространство позволяет использовать возможности познавательных интернет-ресурсов с учетом их доказательственной основы. Критерии использования электронно-цифровых ресурсов в следственной и судебной практике еще только предстоит сформировать и закрепить на законодательном уровне, что обеспечит к ним своевременный и официальный доступ сотрудников правоохранительных органов.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации. – Москва: Проспект, 2021 (по состоянию на 20 февраля 2022 г.).

2. Приговор Дальневосточного окружного военного суда от 9 июля 2019 г., Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 14.01.2020 № 225-АПУ19–4 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 05.09.2022).

3. Постановление Пленума Верховного Суда РФ от 09.02.2012 № 1 (ред. от 03.11.2021) «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 05.09.2022).

4. Приговор Брянского областного суда от 10 июля 2020 года, апелляционное определение судебной коллегии по уголовным делам Первого апелляционного суда общей юрисдикции от 16 декабря 2020 года, Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 03.06.2021 № 83-УД21–17сп-А1 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 05.09.2022).

5. Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2 (утв. Президиумом Верховного Суда РФ 30.04.2020) // Бюллетень Верховного Суда РФ, № 6, июнь, 2020.

Д. Н. Рудов,
кандидат юридических наук, доцент,
Юридический институт Белгородского государственного национального исследовательского университета

К ВОПРОСУ О ПРЕДУПРЕЖДЕНИИ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Аннотация. В статье рассматривается проблема противодействия и пресечения цифровой преступности, порождаемой непрерывной глобализацией и модернизацией современных IT-технологий. Определены основные направления системы предупреждения цифровых преступлений, анализирован практический опыт по противодействию данного вида преступности. Особое внимание уделено профилактическим мерам преступности в рассматриваемой сфере. В заключении автор отметил основные недостатки системы предупредительных мер в сфере борьбы с цифровыми преступлениями.

Ключевые слова: право, цифровизация, цифровые преступления, цифровые технологии, предупреждение преступности

ON THE PREVENTION OF DIGITAL CRIME: THEORETICAL AND PRACTICAL ISSUES

Abstract. The article deals with the problem of countering and suppressing digital crime generated by continuous globalization and modernization of modern IT-technologies. The main directions of the system for the prevention of digital crimes have been determined, practical experience in countering this type of crime has been analyzed. Particular attention is paid to preventive measures of crime in this area. In conclusion, the author noted the main shortcomings of the system of preventive measures in the field of combating digital crimes.

Keywords: Law, Digitalization, Digital crimes, Digital technologies, Crime prevention

Современные цифровые технологи активно входят в нашу жизнь. При этом помимо положительного эффекта в промышленности, торговле, и других сферах жизни указанные технологии способствовало созданию в России нового вида преступности – цифровой преступности. С учетом неготовности ряда слоев населения к быстроменяющейся системе жизнедеятельности цифровизация помимо положительного эффекта в экономике и других сферах жизни несет в себе и ряд угроз, прежде всего, для категории лиц которые более медленно адаптируются современным цифровым технологиям. При этом предупреждение преступлений совершенных с применением цифровых технологий представляет сложную задачу, которая в первую очередь ложится на сотрудников органов внутренних дел и службы безопасности соответствующих структур вовлеченных в деятельность с использованием цифровых технологий. При этом из собственного практического опыта работы в территориальном органе МВД России (СУ УМВД России по г. Белгороду) автору статьи известно о технических сложностях возникающих при предупреж-

дении, раскрытии и расследовании преступлений совершенных с использованием цифровых технологий.

Повышение уровня деятельности сотрудников органов внутренних дел по предупреждению и профилактики преступлений совершенных с применением цифровых технологий влечет за собой повышение затрат государства на техническое оснащение сотрудников полиции и привлечение на работу специалистов высокого уровня. При этом минимальные затраты возможны только при организации повышения квалификации сотрудников органов внутренних дел и соответствующих работников организаций использующих в своей детальности цифровые технологии.

Предупреждение преступлений, совершаемых с использованием высоких технологий (цифровых технологий), является одним из приоритетных направлений деятельности органов внутренних дел [1. С. 60].

Применительно к системе предупреждения высокотехнологичной цифровой преступности можно выделить несколько направлений.

Ни для кого не секрет, что важным направлением противодействия цифровым преступлениям являются социальные меры, так, например, профилактика цифровых преступлений может и должна начинаться с пожилыми лицами, которые только начинают осваивать некоторые виды деятельности с использованием цифровых технологий. Так, в деятельности правоохранительных органов неплохо зарекомендовала себя работа по разъяснению пожилым людям действий при обращении к ним мошенников в рамках «телефонного мошенничества». Здесь необходимо сказать и положительной реакции руководства банковских структур, которые осознают, что массово совершаемые преступления с использованием цифровых технологий подрывают доверие населения и к их деятельности, так как фактически хищения, как правило, совершаются с использованием банковских переводов. Подготовка различных информационных стендов и размещением информации о способах совершения цифровых преступлений, а также бесед сотрудников банковских структур в офисах банковских организаций важный элемент профилактики цифровых преступлений.

Отдельно стоит отметить и способы воздействия на «незащищенные» слои населения при профилактике преступлений совершенных с использованием цифровых технологий, которые предусматривают осуществлением разъяснительной работы во взаимодействии со средствами массовой информации (телевидение, радио, печатные издания).

На наш взгляд, важным элементом предупреждения и профилактики цифровых преступлений будут являться научно-технические меры профилактики преступлений совершенных с использованием цифровых технологий, которые включали бы в себя формирование и государственную поддержку системы целевых фундаментальных и прикладных научных исследований как необходимого элемента научного обеспечения деятельности по профилактики указанного вида преступлений. Система государственной поддержки научных исследований в данном направлении по нашему мнению являлась бы наиболее эффективной формой способствовавшей профилактике и предупреждению преступлений совершенных с использованием цифровых технологий.

При этом мы можем говорить и о расширение сети научно-исследовательских и образовательных учреждений, обеспечивающих разработку научных исследований в сфере высоких технологий и подготовку соответствующих специалистов, а также «целевом» наборе студентов (магистрантов, аспирантов) на соответствующие специальности (направления подготовки).

Необходимо отметить и положительные наработки правоохранительных органов и заинтересованных коммерческих организаций по противодействию преступлениям, совершенным с использованием цифровых технологий.

Так, в целях быстрого получения от кредитных организаций, интернет-провайдеров, операторов связи, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по уголовным делам принимаются меры по совершенствованию механизма взаимодействия следственных органов с оперативными подразделениями, заинтересованными ведомствами и представителями бизнес-сообщества, предусматривающие возможность оперативной блокировки сайтов интернет-пирамид (хайд-проектов), фишинговых сайтов и мошеннических Колл-центров, а также номеров мобильных телефонов, с использованием которых осуществляются хищения денежных средств. В связи этим были заключены соответствующие соглашения с ПАО «Сбербанк» (23.10.2017), Банк ВТБ (ПАО) (25.12.2017) и ПАО «МТС» (30.08.2019), с ПАО «ВымпелКом» (05.12.2019)[1, С. 60].

В целях сокращения фактов цифровых преступлений корыстной направленности, в МВД России создана специализированная база данных «Дистанционное мошенничество», где аккумулируется информация о зарегистрированных IT-преступлениях и устройствах, с помощью которых осуществляются хищения денежных средств. В указанный модуль сотрудниками территориальных органов внутренних дел на региональном уровне вносится актуальная информация о вновь выявленных фактах IT- преступлений.

Однако на данный момент имеются проблемные вопросы ее функционирования, а именно она сформирована не в полной мере.

Согласно сведениям, представленным УОРИ МВД России, массив учтенной информации содержит 141 950 записей о фактах противоправных деяний (номера КУСП или уголовных дел), а также сведения о 166 970 используемых при этом устройствах мобильной связи и 48 647 банковских счетах. К данному массиву имеют доступ более 6 тыс. региональных пользователей, которыми в 2019 г. выявлено 7 603 совпадения по номерам телефонов, фигурирующим в 28 530 уголовных делах, в том числе 296 совпадений по 1 035 банковским счетам и 1 393 совпадения по 3 373 банковским картам [2. С. 12].

Важное значение придается профилактике преступности в рассматриваемой сфере. В рамках профилактической работы особое внимание следует уделять наименее защищенным слоям населения. Целесообразно применять для этого различные способы распространения информации (в органах власти, муниципальных образованиях, государственных, медицинских, образовательных и других учреждениях, на объектах торговли и массового пребывания граждан). Транслировать через СМИ сообщения об успешном расследовании цифровых преступлений, проводить брифинги и пресс-конференции.

На практических примерах разъяснять работу мобильных банковских приложений, предотвращающих дистанционное подключение сторонних лиц путем блокировки возможности восстановления логина и пароля онлайн.

В целях повышения уровня профилактической работы управления общественных связей МВД России разработан, утвержден и реализуется План внешних коммуникаций МВД России и Банка России по противодействию кибер-мошенничеству на 2020 год [3. С. 10]. В нем предусмотрено проведение ряда мероприятий по информированию населения о преступлениях рассматриваемой категории и способах противодействия им, с привлечением ведомственных, региональных и федеральных средств массовой информации.

В качестве положительного примера можно привести опыт деятельности МВД по Республике Башкортостан, где в целях профилактики преступлений и дополнительного информирования населения о новых способах совершения хищения имущества и денежных средств в 2019 г. на региональном сайте МВД размещено 352 материала, интернет-изданиями и интернет-порталами опубликовано 368 материалов, в печатных изданиях – 37, региональными СМИ выпущено 57 видеосюжетов [3.С. 10]. Разработан и утвержден план дополнительных профилактических мероприятий, в рамках исполнения которого на территории республики проводилась соответствующая работа с максимальным привлечением сотрудников территориальных органах внутренних дел.

Таким образом, можно говорить о том, что правоохранительными органами осуществляется достаточно обширный перечень мероприятий, направленный на борьбу с преступлениями, совершаемыми с использованием цифровых (информационно-телекоммуникационных) технологий. Однако задачи, поставленные перед государством по совершенствованию указанного противодействия, решены не в полной мере.

Список литературы

1. Аносов А. В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие. – Москва: Академия управления МВД России, 2019. С. 60.

2. Анализ практики расследования преступлений, совершенных в сфере телекоммуникаций и компьютерной информации: учебное пособие / В. В. Гончаров, В. Ю. Иванов, К. Р. Аветисян, Д. В. Гусев. – Москва: Московский университет МВД РФ им. В. Я. Кикотя, 2020. С. 12.

3. Анализ практики расследования преступлений, совершенных в сфере телекоммуникаций и компьютерной информации: учебное пособие / В. В. Гончаров, В. Ю. Иванов, К. Р. Аветисян, Д. В. Гусев. – Москва: Московский университет МВД РФ им. В. Я. Кикотя, 2020. С. 10.

А. Е. Середа,
ведущий специалист,
учебная лаборатория криминалистической техники и судебных экспертиз,
кафедра криминалистики юридического факультета,
Белорусский государственный университет

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КРИМИНАЛИСТИЧЕСКОМ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ АВТОМАТИЧЕСКОГО РАСПОЗНАНИЯ ЛИЦ

Аннотация. В статье рассматриваются аспекты применения искусственного интеллекта в автоматических системах распознания лиц в рамках поддержания национальной безопасности. Также рассмотрению подвергается такая особенность искусственного интеллекта как «глубокое обучение» и его роль в криминалистическом обеспечении расследования преступлений.

Ключевые слова: криминалистика, искусственный интеллект, глубокое обучение, алгоритмы распознания, распознание лиц, технологии, преступность, национальная безопасность, криминалистическая идентификация, верификация

ARTIFICIAL INTELLIGENCE IN THE FORENSIC USAGE OF AUTOMATIC FACIAL RECOGNITION TECHNOLOGIES

Abstract. The article deals with the issues of ensuring national security through deployment of facial recognition technologies in forensics. It also takes a close look at the emerging trend of utilizing artificial intelligence in this field and aims to unravel the mystery of the so-called Deep learning by focusing on the phenomena being incorporated into facial recognition technologies.

Keywords: Forensics, Artificial intelligence, Deep learning, Algorithms, Facial recognition, Technology, Crime, National security, Identification, Verification

Introduction. The issues of ensuring national security are now becoming increasingly relevant affecting the interests of a wide range of subjects. The volume of information as well as information technologies and the processes of globalization form the conditions under which the world information arena becomes a means of achieving various goals, namely a unique phenomenon and a new sphere of society's day-to-day life. Taking into account the increasing volume and availability of information and information resources, the changing technological landscape of modern society, it seems necessary to take into consideration the challenges and problems unique to our time requiring close attention from the legislative and executive branches of the government.

On the international level, the problem of combating crime is quickly gaining worldwide relevancy and significance. The world economy is being actively transformed and is characterized by increased instability, caused in part by transition to a new technological order. On a global scale, markets are being redistributed, financial flows and productive forces are also being redistributed, and competition is becoming tougher through escalation of interests. Technological evolution is rapidly becoming a source of fundamentally new

threats and opportunities, providing previously inaccessible options for both negative and positive influence on the individual, state, and society in general. Many indicators of crime (dynamics, structure, latency, detection) largely depend on the effectiveness of the fight against professional crime and its prevention, which cannot be fully conducted without the use of modern technological advances.

Successful crime prevention in 2022 is characterized in large part by new strategies and approaches to its implementation. It should be noted that one of the most promising tools for the investigation, solving and prevention of crimes can be the technology capable to strip a perpetrator of his actual or perceived (in case of crime prevention) anonymity. In modern days, the main driving force of crime, in addition to the motive for committing a crime (usually it's greed, jealousy or hatred), is the expectation of the criminal that his identity will remain unknown. Thus, a potential criminal, hiding his identity, eventually commits a felony or misdemeanor (depending on the illegal activity) – as examples of this could be seen the riots and property destruction by mobs in Minsk on August 20, 2020; uprising on the Capitol Hill in the USA on January 6, 2020; riots and damage to property by the Black Lives Matter organization on May 25 in the USA; aggressive protests by truckers on February 12, 2022 in Canada, etc. For the same reason, we can observe an exponential increase in cybercrime around the world, namely perceived or actual anonymity of a perpetrator.

The most effective way to deprive a criminal of his anonymity appears to be the automatic face recognition technology (AFRT). However, in the Russian-language literature, there is almost no analysis of the concepts of face recognition proposed by various researchers – a clear classification of face recognition in the investigation of crimes is not proposed; prospects for further implementation in the investigation of crimes in the future are not offered. All these aspects are extremely important for the current stage of the development of criminalistics.

Main body. Throughout its development, face recognition in criminalistics has gone through several stages of its development: 1) verbal portrait; 2) bertillonage-anthropometry; 3) photo-video technology; 4) automatic recognition by facial characteristics.

In turn, the process of development of automatic recognition by facial characteristics and other signs can also be divided into the following stages of the formation of this technology: 1) quasi-automatic computerized face recognition systems; 2) fully automatic recognition and the emergence of biometric databases of persons for identification; 3) the use of linear algebra to work with images; 4) the implementation of this technology to ensure the safety of public order, disclosure and investigation of crimes; 5) the development and use of numerous algorithms in the development of automatic face recognition systems; 6) 3D face recognition and artificial intelligence [1. P. 16–17].

Over the past 10 years, the use of automatic face recognition technology in video surveillance systems has become increasingly common worldwide. In total, there are currently 109 countries that either use or have approved the use of facial recognition technology for surveillance purposes. Since the development of automatic face recognition systems, much attention has been paid to its further progress and implementation into the technological and scientific landscape of society by such foreign authors as Mark Kempster, Alberink, Ruyfork, Desmoz, Champode, Messer, Harley, Chunk, etc.

Kempster considers face recognition in the context of law enforcement and gives the following definition: «Face recognition is an activity aimed at assimilating information that is hidden in the general set of facial features of an individual. This information can be read and recorded by giving mathematical and graphic design of the presented features and characteristics of the person, which, in their separate state, do not represent information significant for identification of the individual, but in their totality, are the business card of the individual». According to this point of view, face recognition is a unifying process, which consists in giving a system to separately presented features, which together represent identifying information. This approach is extremely common and it was this point of view that formed the basis of the first semi-automatic face recognition systems [1. P. 31–32].

Alberic and Ruyfork see face recognition as a process of presenting the received information in a graphical form and further identifying a person, drawing an already thin line between the two concepts. Face recognition, in this case, is the process of identifying the correspondence of the characteristic features and features inherent in the face to the already available and graphically presented characteristics of the face for comparison. Simply put, this point of view reduces two different processes: recognition and identification of a person to a single process [5, P. 42–43].

Dezmoz positions face recognition as a process of fixing and mathematically displaying static and dynamic characteristics of a face. This approach is due to the fact that the researcher sees identifying signs in such dynamic characteristics as blinking, lip movement, nervous twitching or rolling of the eyes, narrowing and widening of the nostrils, etc. «Face recognition», stipulates the researcher, «is not possible without fixing and displaying all signs without exception: including dynamic ones, which, for the most part, are unique to humans» [5. P. 46–49].

In the position of the researcher, it is clearly expressed that he operates from the point of view of the latest technologies – automatic face recognition systems. We believe that the recognition of dynamic facial features seems to be an appropriate aspect of face recognition and, of course, will be of great interest for the detection and investigation of crimes.

Champod, developing his approach in collaboration with Dezmoz, proposed his own classification of signs for recognition: 1) signs of belonging – belonging to race, nation, gender, etc. 2) identifying (or unique) signs – forehead height, eye color, mouth width, scars, etc. Further, the researcher recommends dividing the signs into 1) general – the largest elements, such as: figure, clothing size, hair color; 2) private – these are components of the general signs that their detail; 3) permanent signs (define individual traits); 4) temporary (tan, tattoos, hair, teeth, etc.); 5) accidental (traces of diseases, skin pigmentation, acne) [6. P. 87–88].

Messer and Harley argue that face recognition is always a semi-automatic process, carried out not without the participation of a specialist in the respective field and computer technology (in the case of face recognition, biometric databases and the algorithm used in the recognition process). In recognition using modern technologies, researchers distinguish 3 main stages: 1) preliminary – reading and fixing of information; 2) intermediate – loading of the received information into the database for identity search; 3) final – control verification of the result by an expert. Obviously, Messer and Harley took as a basis the position of Alberink and Ruyfork that face recognition includes the final identification of a face – the difference is that they focused on systematization of the process, highlighting the need for the participation of a specialist at the final stage of face recognition [8. P. 277–280].

Chunk pointed out the need to include in the concept of «Face recognition» such an element as a dynamic change in the features of the external appearance of the face, its characteristic properties and features in the aging process. At its core, the researcher, taking into account the technological development and the increase in the capabilities of modern algorithms for automatic face recognition, expands the concept itself. Face recognition, according to him, not only consists of fixing and processing the data available at the time of reading the information, but also the use of artificial intelligence, whose task is to predict how much the appearance of this person will change in the future, or how his face looked in the past. Thus, according to Chunk, it will be possible to uncover and investigate crimes of considerable prescription, as well as to predict in advance what a potential criminal will look like in the future, which will greatly simplify the achievement of the ultimate goal of face recognition –identification of the criminal [8. P. 211–212].

According to the American criminology researcher Richard Seiferstein, facial recognition technology is a form of biometric artificial intelligence (AI) that performs identity verification by comparing video frames or digital images and matching them with images of faces stored in a database based on facial features and skin texture. It provides automatic, fast and unhindered verification, since no physical contact, such as fingerprints or other security measures, is required. In addition, it is not related to any keys or identity cards that may be stolen or lost.

At the current stage of development, researchers agree that face recognition in the form in which it exists as of 2022 is a revolutionary technology, one of the important components of which is Deep learning.

Deep learning is a type of Machine learning and artificial intelligence (AI) that simulates how people acquire certain types of knowledge. Deep learning is an important element of data science, which includes statistics and predictive modeling. In its simplest form, Deep learning can be considered as a way to automate predictive analytics. While traditional Machine learning algorithms are linear, Deep learning algorithms are built into a hierarchy of increasing complexity and abstraction.

In traditional Machine learning, the learning process is controlled, and the programmer must be extremely precise, telling the computer what types of objects he should look for in order to decide whether an image contains a particular object. This is a time-consuming process called «Function extraction», and the success of the computer depends entirely on the programmer's ability to accurately determine the set of functions. The advantage of Deep learning is that the program itself creates a set of functions without human supervision [2].

Investigating the issues related to the use of technical and forensic tools in the context of general aspects of fixing evidence in criminal proceedings, scientists note that the tools used are not just auxiliary in working with evidence, contributing to their capture and preservation. For example, in accordance with the opinion of A. A. Levy, video recording with face recognition «performs an essential cognitive function, to a certain extent replaces the court's direct perception of recorded information»

However, face recognition may have a different definition depending on the method, object and purpose of recognition. Van der Lugt, a researcher of automatic face recognition systems, pointed out that face recognition by a person, technology with human participation, or

fully automatic face recognition does not fall under the same category of face recognition and, therefore, should be considered different in its essence and nature processes [10. P. 115–118].

In the same vein, David Kuhn emphasizes, we can talk about the nature of the activity in which facial features and characteristics are recognized. The researcher adheres to a certain dichotomy in this matter: the recognition of a face, its dynamic and static features, can be carried out within the framework of law enforcement activities (investigation of crimes, as well as their prevention), as well as within the framework of maintaining security (face recognition in electronic devices, for admission to a limited territory, etc.) [11. P. 65–68].

In addition, it also seems to us extremely important to highlight a distinction between the concepts of «Identification» and «Verification» – both concepts are important to the study, application and legislative consolidation of automatic face recognition technology, since, as a result of the study of automatic face recognition technology, at the present stage, the result of face recognition is always one of the following: face verification, identification, or recognition of emotions.

Verification of a person, in this regard, is the result of the congruence of the biometric characteristics of the person captured in the photo with the characteristics of the person stored in the database. In other words, the comparison and search for matches of biometric characteristics of the same person in the photo and in the available database is carried out. In case of positive verification, access to a place is provided, a service is provided, etc. [7. P. 96–97].

Identification of a person is fundamentally different from verification. Identification of a person by biometric characteristics of a person consists in finding matches of the facial portrait compiled by the algorithm of the face recognition program with numerous others presented in the database. We are talking about establishing the identity of a suspect, victim, accused or other participant in the criminal process, as well as missing persons or victims of an accident [7. P. 91–92].

As of 2022, the main array of automatic face recognition systems consists of 2D (two-dimensional) recognition systems. The 2D facial recognition technology is based on flat two-dimensional images. Face recognition algorithms use: anthropometric parameters of the face, graph models of faces or elastic 2D models of faces, as well as images with faces represented by a certain set of physical or mathematical features. 2D image recognition is one of the most popular technologies at the moment. Since the main databases of identified persons accumulated in the world are precisely two-dimensional, the main equipment already installed around the world is predominantly 2D.

However, the development and implementation of 3D scanning and facial recognition systems is already underway. 3D recognition is usually performed in a reconstructed three-dimensional way. This type of facial recognition technology has higher quality characteristics. There are several different 3D scanning technologies: these can be laser scanners with an estimate of the range from the scanner to the elements of the object's surface, special scanners with structured illumination of the object's surface and mathematical processing, or they can be scanners that process photogrammetric synchronous stereo pairs of images of faces.

Automatic face recognition includes several stages [4]:

1. Face detection. The camera will detect a person's face, whether he is alone or in a crowd. The face is more effectively detected at the moment when a person looks

directly into the camera; however, modern technological advances make it possible to detect a face in situations when a person is not looking directly (within certain limits).

2. Face analysis. When a photo of the face has been taken, its analysis begins. Most face recognition solutions use 2D images instead of 3D volumetric images, because they can more easily match 2D photos with publicly available photos or photos available in a database. Each face is made up of distinguishable landmarks or nodal points (such as the distance between the eyes or the shape of the cheekbones). Face recognition programs analyze these nodal points in depth.

3. Converting images to data. After that, the result of analysis of the face turns into a mathematical formula. Facial features become a numeric code. Such a numeric code is called a «Faceprint». Like the unique structure of a thumbprint, each person has their own «Faceprint».

4. Search for matches. Then the received code is compared with photos with IDs in the database.

Modern face recognition technologies, namely their effectiveness is measured by two indicators [5. P. 114–115]:

1) The level of erroneous confirmations (hereinafter referred to as FAR) is the probability that the facial recognition system mistakenly identifies an unregistered user or confirms his authenticity

2) The level of erroneous failures (hereinafter referred to as FRR) is the probability that the system does not identify the registered user or does not confirm his authenticity.

The FRR calculation formula looks like this:

$$\text{FRR} = \frac{FR}{N_t}$$

Where is the number of image standards in the database. FR is the number of false non-recognitions.

FAR is calculated similarly

$$FAR = \frac{FA}{N_T}$$

Where is the number of image standards in the database. FA is the number of false recognitions.

Table 1 shows these indicators for automatic face recognition systems in 2D and 3D format. Based on these indicators, it is preferable to choose a system for certain purposes. Of course, it seems rational to opt for the system with the best indicators (table 1) [5. P. 120–122].

Table 1. Comparison of FAR and FRR indicators for automatic face recognition systems in 2D and 3D format

Approach	False pass ratio (FAR)	False failure rate (FRR)
3D face recognition	0.0005 %	0.1 %
2D face recognition	0.1 %	2.5 %

The first and most important thing to note is that the indicators given in the table are not absolute, but relative, i. e. they may vary depending on the settings of the facial recognition algorithm. The second is that these indicators are interrelated – the smaller the FAR, the greater the FRR. The approximate values of FRR and FAR for facial recognition systems and their relationship are presented below (table 2) [5. P. 125].

Table 2. The relationship of the FAR and FRR coefficients for automatic face recognition systems

FAR	FRR
0.1 %	2.5 %
0.01 %	7 %
0.001 %	10 %

The main disadvantages of 3D facial recognition technology include the following aspects [5. P. 171]:

1) 3D recognition requires special cameras for scanning, which are several times more expensive than conventional CCTV cameras that are used in 2D recognition;

2) lack of ready-made databases of identified persons, compared to 2D recognition;

3) recognition of twins remains a difficult task for facial recognition algorithms. On average, 13.1 twins per 1000 newborns are born in the world, and this figure varies greatly depending on the geographical region.

As of 2022, forensic facial recognition systems are used to track criminals and identify wanted or missing persons. To demonstrate the full breadth of the scale, several examples should be given [2, 3, 4]:

1) By the end of 2018, there were about 4,000 surveillance cameras installed in Minsk as part of the Republican Public Security Monitoring System. In order to maintain law and order, a Synesis product called «Kipod» is used, which allows setting up a biometric system for identification and recognition of persons, as well as identification and recognition of vehicle numbers;

2) In Moscow, as part of the Safe City program, one of the world's largest face recognition networks operates – more than 200 thousand video surveillance cameras. This contributed to the disclosure of more than 5 thousand crimes in 2020. In addition, it was found that the effectiveness of video surveillance systems in solving crimes has an annual increase of 15–16 %;

3) In the People's Republic of China, as of 2018, 170 million surveillance cameras were installed and put into operation, and in the period from 2018 to 2021, another 400 million units were installed. The «Dragonfly Eye» facial recognition system is used to maintain public order. In the first three months of using this technology in Shanghai, law enforcement officers detained 567 criminals, and the level of pickpocketing in the cities where it was implemented fell by almost a third. The Zhengzhou City police, for example, use glasses with a face recognition system that give out a person's name and address in 2–3 minutes.

4) In the United States of America, the facial recognition system «FACES» (a system for comparing and examining faces) is used, which is based on algorithms that scan more than 30 million images from driver's licenses and photos. As of 2022, out of 24 US agencies, 18 already use facial recognition technologies, some use more than one system.

In 2014, Facebook (The Facebook in Russia is recognized as extremist and banned.) launched the «DeepFace» service, which determines whether two photographed faces belong to the same person with an accuracy of 97.25 %. In 2015, Google introduced its development – «FaceNet», which achieved a record accuracy of 99.63 % due to the huge array of data collected by Google services. The technology, in particular, is used in «Google Photos» to sort images and automatically mark people on them [3].

On September 12, 2017, Apple introduced «Face ID» technology, replacing the fingerprint sensor «Touch ID». The technology developed by Apple is unique in the sense that it contains the following elements: 1) a dot projector – it projects more than 30,000 invisible infrared dots onto the user's face, using which his mathematical model is then created; 2) an infrared camera – reads the point structure of the face, creates an image in the infrared spectrum and places this data into a special processor module; 3) infrared emitter – emits an invisible beam of infrared light on the face, which allows one to perform an accurate scan of it even in complete darkness [3].

In addition, companies such as Clearview AI, Vigilant Solutions and Acuant FaceID are also working on their face recognition systems. The enormous amount of information collected by the private sector can be useful for law enforcement agencies, since government agencies have many channels of access to corporate data. In 2020, from January to June alone, federal, state and local law enforcement agencies in the United States sent more than 112,000 legal requests for data to Apple, Google, Facebook and Microsoft – three times more requests than in 2015 (of which approximately 85 % were accepted and responded to) [9].

According to the study «Facial Recognition Market», there are the following algorithms for automatic face recognition (table 3) [3]:

Table 3. The most common, as of 2022, algorithms of automatic face recognition systems in the world

Algorithm	Manufacturer	Country of origin
megvii-000	Megvii	China
visionlabs-003	VisionLabs	Russia
visionlabs-002	VisionLabs	Russia
morpho-002	Morpho	France
morpho-000	Morpho	France
ntechlab-003	NtechLab	Russia
ntechlab-002	NtechLab	Russia
cogent-000	Gemalto Cogent	USA
vocord-002	Vocord	Russia
fdu-000	Fudan University	China
fdu-001	Fudan University	China
neurotechnology-003	Neurotechnology	Lithuania
itmo-003	ИТМО University	Russia
3divi-001	3DiVi Inc.	Russia
yitu-000	Yitu Technologies	China
gorilla-000	Gorilla Technology	Taiwan
cyberextruder-002	CyberExtruder	USA

As of 2022, the regional application of automatic face recognition technology is as follows [3]:

1) Half of North American countries currently use automatic facial recognition technology (50 %);

2) In South America, the vast majority of countries use automatic face recognition technology (92 %);

3) The countries of the Middle East and Central Asia largely use the technology of automatic face recognition (76 %);

4) More than half of European countries currently use automatic face recognition technology (69 %);

5) The smallest number of countries use facial recognition technology in the investigation of crimes (20 %).

Conclusion. The concept of face recognition is quite deep for the reason that it implies a multi-level structure, each element that corresponds or corresponded to the truth at a particular stage of technology development. Currently, based on modern research and the works of authors developing this issue, the following seems to us to be the correct definition of this concept: «Face recognition in criminalistics is an automatic, semi-automatic or manual process aimed at assimilation of information (static or dynamic features) that is hidden in the total set of facial features of an individual. This information can be read and recorded by giving mathematical and graphic design of the presented features and characteristics of the person, which, in their separate state, do not represent information significant for identification of the individual, but in their totality, are a reliable identifier of the individual».

As of 2022, face recognition systems begin to deploy AI algorithms and Machine learning (also known as Deep learning) to detect human faces. The algorithm typically starts by searching for human eyes, followed by eyebrows, nose, mouth, nostrils, and iris. Once all the facial features are captured, additional validations using large datasets containing both positive and negative images confirm that it is a human face. Some of the common techniques used for facial recognition are feature-based, appearance-based, knowledge-based, and template matching. Each of these methods has its advantages and disadvantages.

Feature-based methods rely on features such as eyes or nose to detect a face. The outcomes of this method could vary based on light. Further, appearance-based methods use statistical analysis and Machine learning to match the characteristics of face images. In a knowledge-based approach, a face is recognized based on predefined rules. Template-matching methods compare images with previously stored face patterns or features and correlate the results to detect a face. However, this method fails to address variations in scale, pose, and shape.

Machine learning/Deep learning is a subset of AI that mainly focuses on using data and algorithms to mimic human natural learning processes. It uses statistical methods to train algorithms to classify or predict and even provide insights into data mining projects. Terms like Deep learning and Machine learning and sometimes neural networks are used in the industry interchangeably. However, there are subtle differences between these technologies. A neural network is a subset of Deep learning while Deep learning is one

of the arms of Machine learning. Simply put, Deep learning involves training algorithms with minimal human intervention. It converts unstructured data to manageable groups for processing through a process known as dimensionality reduction.

On the other hand, neural networks also known as artificial neural networks comprise node layers – an input layer, multiple hidden layers, and an output layer. Each of the nodes has an associated weight and threshold and is connected to the other nodes. Basically, if the value of any output layer exceeds its threshold, data is sent to the next layer of the network. Neural networks are of two types: basic neural networks and Deep neural networks. In the basic neural network, two or three layers are present whereas a deep neural network consists of more than three layers.

Artificial Intelligence and Machine learning offer a multitude of opportunities and endless possibilities to work for the betterment of the world. However, it is essential to pay attention to the ethics and privacy of people while dealing with data. Data storage, management, and security are the other aspects that will play an important role in making these technologies invasive. In order to overcome the problematic aspects of the use of facial recognition technology in the detection and investigation of crimes that are relevant as of 2022, it is necessary:

1. Improving the accuracy and reliability of facial recognition systems in the detection and investigation of crimes. To achieve this goal, it is advisable to implement:

– the installation of a larger number of video surveillance cameras, with a high resolution of video recording, a large amount of memory and capable of recording in low light conditions or bad weather. In addition, a single format for recording information should be established;

– development of algorithms for recognizing persons who work equally effectively with representatives of different races and nationalities.

2. Modernization of the privacy and data security infrastructure, which will require:

– installation or development of software that will reliably protect the received data;

– the development of a regulatory legal act of the concept of protection and processing of biometric data providing for responsibility for failure to ensure security in this matter.

3. Development of relevant regulatory legal acts regulating the use of facial recognition technology in integration with existing databases. It is necessary to develop a legal framework that will regulate in detail the use of the interaction of these systems in the investigation and prevention of crimes.

4. Development of training programs for specialists in the field of facial recognition. It is of paramount importance to develop and ultimately deploy training programs for specialists in the field of working with up-to-date face recognition technologies and devising new, more advanced algorithms. As well as there is forensics and counter-forensics, face recognition systems meet their opponents in the form of various kinds of tricks and fakes (for example, the notorious «Deepfake»), as well as means and methods of hiding the characteristic properties of appearance. Up-to-date knowledge of specialists working with facial recognition systems and developers of new algorithms for these systems will allow investigating and solving crimes most accurately and with minimal time costs.

5. Adaptation of algorithms to changes in the appearance of the aging process, as well as surgical interventions and other deformities of the face. The variability of the signs of the suspects, for the most part, implies age-related and surgical changes.

Taking into account the fact that some changes can radically transform a person's appearance, the following is advisable:

1) creation of data banks related to gender, age and ethnicity which provide background information for a variety of diagnostic, clinical and judicial procedures;

2) development and use of an algorithm that is able to take into account the approximate age change of a person after a certain time.

Elements with a bone base, such as the skull, forehead, do not undergo serious changes throughout a person's life. However, the nature of their transformation can mainly be assessed by experts with significant experience or specially developed software algorithms.

References

1. Colmenarez, A. Facial Analysis from Continuous Video with Applications to Human-Computer Interface / A. J. Colmenarez, Z. Xiong, T. S. Huang. – Kluwer Academic Publishers, New York, Boston, 2004. – 159 p.

2. Face off. Law Enforcement Use of Face Recognition Technology. URL: https://www.eff.org/files/2019/05/28/face-off-report.pdf (дата обращения: 11.07.2022).

3. Facial Recognition Market Size, Share & Trends Analysis Report by Technology (2D, 3D, Facial Analytics), by Application (Access Control, Security & Surveilance), by End-use, by Region, and Segment Forecasts, 2021–2028. URL: https://www.grandviewresearch.com/industry-analysis/facial-recognition-market (дата обращения: 14.07.2022).

4. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. URL: https://edpb.europa.eu/system/files/2022–05/edpb guidelines_202205_frtlawenforcement_en_1.pdf. (дата обращения: 12.07.2022).

5. Lambert, W. Issues with Facial Recognition Technology / W. Lambert. – Nova Science Publishers inc., 2022. – 232 p.

6. Lee-Morrison, L. Portraits of Automated Facial Recognition. On Mechanic Ways of Seeing the Face / L. Lee-Morrison. – Majuskel Medienproduktion GmbH, Werzlar, 2019. – 199 p.

7. Lyle, D. Forensics / D. Lyle. – Fraser Direct, 100 Armstrong Avenue, Georgetown, Canada, 2008. – 494 p.

8. Rattani, A. Selfie Biometrics. Advances and Challenges / A. Rattani, R. Derakhshani, A. Ross. – Zillow inc., Seattle, 2020. – 377 p.

9. Racial Discrimination in Face Recognition Technology. URL: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ (дата обращения: 12.07.2022).

10. Saferstein, R. Criminalistics. An introduction to Forensic Science / R. Saferstein, R. Tiffany. – Mt. Laurel, New Jersey, 2020. – 577 p.

11. Vatsa, M. Deep Learning in Biometrics / M. Vatsa, R. Singh, A. Majumdar. – Taylor&Francis Group, LLC, 2018. – 329 p.

Т. В. Стукалова,
кандидат юридических наук, доцент кафедры
уголовно-процессуального права,
Приволжский филиал Российского государственного
университета правосудия

АКТУАЛЬНЫЕ ВОПРОСЫ ЦИФРОВИЗАЦИИ УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В РОССИИ И ЗА РУБЕЖОМ

Аннотация. В рамках данной статьи автор ставил себе целью исследование актуальных вопросов цифровизации российской и зарубежной уголовно-процессуальной сферы. По результатам исследования приходит к выводу о том, что российская уголовно-процессуальная сфера отстает от ряда зарубежных государств, включая государства бывшего СССР, в плане перехода к новым моделям, основанным на информационных технологиях в сфере уголовного процесса. Кроме того, в статье рассмотрены некоторые актуальные возможности цифровизации отдельных направлений уголовно-процессуальной деятельности.

Ключевые слова: цифровизация, уголовный процесс, расследование преступлений, искусственный интеллект, электронное уголовное дело, информационные технологии, полиробот-прокурор

TOPICAL ISSUES OF DIGITALIZATION OF CRIMINAL PROCEDURAL ACTIVITY IN RUSSIA AND ABROAD

Abstract. Within the framework of this article, the author aimed to study the consideration of topical issues of digitalization of the Russian and foreign criminal procedure sphere. Based on the results of the study, the author comes to the conclusion that the Russian criminal procedure sphere lags behind a number of foreign states, including the states of the former USSR, in terms of transition to new models based on information technologies in the field of criminal procedure. In addition, the article discusses some current opportunities for digitalization of certain areas of criminal procedural activity.

Keywords: Digitalization, Criminal process, Investigation of crimes, Artificial intelligence, Electronic criminal case, Information technology, Polyrobot prosecutor

В процессе формирования и становления постиндустриального общества все большую роль в современном государстве играют научные достижения, связанные с использованием актуальных информационных технологий. В настоящее время цифровизация пытается охватить все сферы жизнедеятельности российского общества и государства.

В соответствии с представленными экспертными заключениями [18] Россию пока еще сложно считать цифровым государством, поскольку цифровизация затронула еще не все сферы жизнедеятельности и не в полноценном объеме. Так, ведущими странами-лидерами перспективной цифровой экономики и других сфер жизнедеятельности выступают Швеция, Норвегия и Швейцария. Российская Федерация

находится на тридцать девятом месте цифрового рейтинга, где главенствующее место отведено в современный период таким странам, как США, Великобритания, Южная Корея, Гонконг и Дания.

Учитывая мировые высокодинамичные процессы цифровизации, необходимо разрабатывать и внедрять российскую модель виртуального пространства. Такая цифровая система должна охватить и сферу правоохранительных органов при реализации функции привлечения к уголовной ответственности. Множество экспертов и ученых-специалистов в области уголовных, уголовно-процессуальных и уголовно-исполнительных отношений признают необходимость создания матрицы цифрового правосудия [15. С. 120]. При внедрении цифровизации в правоприменительную деятельности необходимо отграничивать рассматриваемое явление от информатизации [13].

В рамках уголовно-процессуальной деятельности многие направления при грамотном и рациональном подходе можно цифровизировать. В частности, особый интерес вызывают роботы-прокуроры и роботы-судьи. На наш взгляд, лучше применять термины полироботы. Интересен опыт Китая. В Китайской Народной Республике разработана программа искусственного интеллекта, осуществляющая функцию прокурора по предъявлению обвинения [19]. Следует отметить, что китайские нейропрокуроры формулируют (выдвигают) обвинение с точности до 97 % [5].

Необходимо подчеркнуть, что технологии искусственного интеллекта используются и в Европейском Суде по правам человека [3]. В 2016 г. компьютер с искусственным интеллектом смог в рамках эксперимента проанализировать около шестисот дел, находящихся в производстве Суда. Параллельно с программой-роботом дела изучали и старшие компетентные судьи Суда. По словам разработчиков рассматриваемой программы процент точности принятия и обоснования решения программой составил 79 %. Интересно то, что в программу была заложена задача решения не только вопросов юридических доказательств, но и задача решения этических вопросов [9].

Примечателен и опыт Франции [8] в использовании цифровизации правосудия. Так в апреле 2018 г. в Совете министров Франции был представлен законопроект о программировании правосудия на 2018–2022 гг. В рамках реализации данной программы было предложено разгрузить судебную систему путем введения максимальной замены деятельности судей цифровыми технологиями. Так, программы-роботы предлагали спорящим сторонам (в основе правовой эксперимент был направлен на решений гражданских и административных споров) возможные способы разрешений конфликта по имеющейся правоприменительной практике (без участия судьи). Кроме того, такая процедура решения спора рассматривалась как внесудебная (досудебная). Такая программа позволила: снизить нагрузку на действующих судей, оперативно (в короткие сроки) разрешать споры (конфликты), сократить финансовые расходы на производство, и др. При этом задачей государства являлось широкое и активно применение видеоконференц-связи с целью разрешения конфликта мирным (досудебным, субсидиарным, вспомогательным) путем. Следует подчеркнуть, что реализация анализируемого французского законопроекта затронула на первом этапе более двух с половиной млн дел.

В США [17] в 2017 г. был также проведен интересный эксперимент, в рамках которого программы-роботы проанализировали решения Верховного Суда США за период с 1816 г. по 2015 г. с точностью предсказания более 70 %. Всего искусственным интеллектом было проанализировано около 30 тыс. дел.

Проблеме создания полироботов-судей также уделяется в современный период много внимания [1]. Создание и внедрение полироботов-прокуроров и полироботов-судей вызывает с достоверной необходимостью переход на систему электронных уголовных дел [16]. Электронный вариант уголовного дела будет гораздо более простым в обслуживании искусственным интеллектом.

Введение в судопроизводство электронных уголовных дел – это вопрос времени. Вместе с тем на сегодняшний день говорить о повсеместном введении электронных уголовных дел рано, более того представляется, что данный процесс не должен быть перманентным. Постепенно отдельные элементы системы электронных уголовных дел будут вводиться в судах, будет совершенствоваться система организационно-технического обеспечения уголовного судопроизводства. При этом крайне важно обеспечить высокую степень защищенности данных, размещаемых в рамках электронных уголовных дел и построить эффективный механизм защиты от возможных фальсификаций.

Следует обратить внимание, что во многих государствах мира уже системы ведения электронных судебных дел применяются ни один год. Например, в Бельгии в 2005 г. был создан проект электронного правосудия Phenix, в рамках которого, помимо системы электронного документооборота судов, «электронный файл» мог пополняться полицией, адвокатом, сторонами. Вопрос аутентификации решался при помощи электронного паспорта. В Саудовской Аравии уголовное судопроизводство по многим делам заканчивается в течение всего нескольких дней. В этой стране судебные органы начали вести электронные уголовные дела несколько лет назад, тем самым сократив сроки расследования на 80 %. В Азербайджане при расследовании налоговых преступлений применяется программа «Электронное уголовное дело» уже с 2016 г.

В соответствии со ст. 42.1 Уголовно-процессуальный кодекс Республики Казахстан от 04.07.2014 № 231-V (с изменениями и дополнениями по состоянию на 03.09.2022 г.) [14] уголовное дело может вестись в бумажном и (или) электронных форматах.

Порядок осуществления уголовно-процессуальной деятельности с использованием электронных форм документооборота в большей степени регулируется приказом Генерального прокурора Республики Казахстан от 03.01.2018 № 2 «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате» (с изменениями от 15.02.2021) [11]. В Инструкции изложены основные понятия, которые используются при расследовании преступления в формате электронного документа, а также порядок и особенности электронного досудебного производства.

Основная проблема возможности введения электронных судебных дел – это проблема фальсификации материалов электронного судебного дела, где определенный субъект (будь то человек, неправомерно получивший доступ к электронным

базам данных судов, или же какое-либо должностное лицо, к примеру, работник суда) может осуществить фальсификацию материалов электронного дела, или же «украсть» информацию, составляющую установленную законом тайну (личную, служебную, государственную и т. д.). С учетом данного обстоятельства ключевым аспектом ведения электронных судебных дел должно быть построение эффективной защиты данных, которые содержатся в указанных делах.

Многие ученые в области уголовно-процессуальной доктрины [12] свидетельствуют о технологической отсталости российской уголовно-процессуальной деятельности. Это, в свою очередь, является препятствием цифровизации и модернизации российского уголовного процесса.

Следующая проблема имеет организационно-технический характер, а именно в настоящее время далеко не все суды имеют соответствующее техническое оснащение, которое бы позволяло им вести электронные уголовные дела, т. е. формировать материалы электронных дел, взаимодействовать с заявителями и иными органами государственной власти в электронной форме и т. д. Помимо этого совершенно очевидно, что для формирования электронных дел следует разработать специальный программный комплекс с одновременной подготовкой кадров, умеющих работать на таком программном оборудовании. Немаловажной проблемой является и наличие технических сбоев при функционировании системы электронных уголовных дел (систематические технические сбои, перегрузки серверов, различного рода технических ошибки, и др.).

Что же касается положительных моментов введения электронных уголовных дел, то они очевидны: серьезным образом упроститься взаимодействие между органами судебной власти и иными органами, организациями и гражданами; сократятся бумажные и канцелярские расходы; электронные данные легко копировать, делать рассылку и т. д.

Говоря об искусственном интеллекте (полироботах-прокурорах, полироботах-судьях, и др.), не стоит забывать, что самым главным условием принятия процессуального решения в рамках производства по уголовному делу, должна стать ответственность человека. Следовательно, абсолютно все решения, принимаемые полироботизированными программами, должны проходить обязательный человеческий контроль. Существование такого контроля позволит решить множество задач: предоставит возможность реализовать принцип свободы оценки доказательств; позволит свести к минимуму или исключить технические, юридические и этические ошибки; разрешит реализовать принцип персонализации ответственности за принятое процессуальное решение, и др.

Следовательно, возможности использования систем цифровизации, включая систем искусственного интеллекта, в уголовно-процессуальной деятельности многообразны и вариативны. Цифровизация правотворческой и правоприменительной систем современных государств мира – это только вопрос времени.

Следовательно, искусственный интеллект, на наш взгляд, должен принимать участие в процессе принятия процессуального решения, где требуется комплексное, всестороннее мышление: решение процессуального вопроса о возбуждении уголовного дела (либо об отказе); решение процессуального вопроса о предъявлении

обвинения (о привлечении в качестве обвиняемого) или уведомления о подозрении; решение вопроса об окончании предварительного расследования и констатации факта о проведении всестороннего и объективного расследования и доказанности всех обстоятельств, входящих в общий и специальные предметы доказывания; решение вопроса об утверждении обвинительного заключения; решение вопроса о готовности уголовного дела к рассмотрению в судебном разбирательстве по первой инстанции; итоговое решение (приговор или иное) суда первой, апелляционной, кассационной, надзорной инстанций, и др.

Необходимо отметить, что общественные отношения с использованием искусственного интеллекта требуют предварительного правового регулирования [10]. В связи с этим особое внимание следует уделить правотворческой деятельности с учетом цифровизации [2]. В современный период возросла значимость использования цифровых технологий в сфере анализа мыслительной деятельности человека в процессе создания нормативных правовых актов. Особенно интересным, на наш взгляд, считаем использование технологии блокчейн [4]. Компьютерные технологии в ближайшем будущем должны стать средством регулирования общественных отношений. Ряд ученых предлагают закодировать общественные отношения (присвоить коды в зависимости, например, от сферы жизнедеятельности). Затем разработать компьютерные программы, подготавливающие законопроекты отдельных нормативных правовых актов и определяющие приоритет и перспективы государственной политики в области законопроверческой деятельности. Такие компьютерные технологии позволят автономно (без участия человека) осуществлять правотворческие функции. В рамках использования технологий блокчейн произойдет: автоматизация отдельных этапов (стадий) правотворчества, включая определение сферы, требующей немедленного нормативного совершенствования (правовой корректировки); подготовка законопроектов с использованием машиночитаемых норм, и в результате принятие нормативных правовых актов с использованием современных технологий (сводя к минимуму деятельность человека). Процесс правотворчества может превратиться в определенный алгоритм (закрепление различных последовательностей операций).

Ученые-специалисты предлагают в рамках технологии блокчейн применять принцип смарт-контракта (принцип компьютерного алгоритма, предназначенного для процесса формирования, осуществления контроля и предоставления информации об этом соответствующим субъектам о владении чем-либо). В более узком смысле под смарт-контрактом понимается комплекс данных в текущем состоянии и набор функций, находящихся по определенному адресу в блокчейне. Таким образом, предлагается в правотворческой деятельности применять компьютерный код для регулирования сферы определенных общественных отношений. Разработка специального языка программирования с последующим аудитом такого кода (внешним и внутренним) позволит сделать правотворческую деятельность целесообразной и эффективной. Все перечисленное позволит осуществить прозрачность кода и доступность информации к нему.

В рамках правотворческой деятельности необходимо переработка уголовно-процессуального законодательства и корреспондирующей нормативной правовой базы с учетом цифровизации уголовно-процессуальной деятельности. В частности, необходимо внести изменения в ст. 5 УПК РФ, отразив в указанной статье следую-

щие понятия: «Единый реестр досудебных расследований» (ЕРДР), «Электронное уголовное дело», «Электронная цифровая подпись», «Электронный документ» и др. Кроме того, должны быть изменены и дополнены другие нормы УПК РФ, исходя из общей государственной концепции цифровизации уголовного процесса.

В развитие идей цифровизации уголовно-процессуальной деятельности необходимо, на наш взгляд, предложить создание технологических программ, своего рода полироботов-следователей и полироботов-дознавателей. Такие программы могут использоваться на самых сложных этапах предварительного расследования. Например, для составления итогового процессуального документа при окончании предварительного расследования (обвинительное заключение, обвинительный акт, обвинительное постановление).

Наличие искусственного интеллекта в уголовно-процессуальной деятельности позволит эффективно реализовывать принципы уголовного процесса, особенно принцип разумного срока уголовного судопроизводства, принцип процессуальной экономии, принцип обеспечения прав и свобод личности.

Говоря об искусственном интеллекте, не стоит забывать, что самым главным условием принятия процессуального решения в рамках производства по уголовному делу должна стать ответственность человека. Следовательно, абсолютно все решения, принимаемые полироботизированными программами должны проходить обязательный человеческий контроль. Существование такого контроля позволит решить множество задач: предоставит возможность реализовать принцип свободы оценки доказательств; позволит свести к минимуму или исключить технические, юридические и этические ошибки; разрешит реализовать принцип персонализации ответственности за принятое процессуальное решение, и др.

Одним из главных аспектов, который может вызвать деятельность по использованию искусственного интеллекта во всех сферах жизнедеятельности, на наш взгляд, выступает этика искусственного интеллекта. В современный период достаточно много исследований [7] посвящено этике искусственного интеллекта. Следует отметить положительный момент, заключающийся в том, что современный уровень развития науки позволяет, во-первых, вести речь о проектировании этически обусловленных систем искусственного интеллекта. Во-вторых, поставленная задача может быть решена уже в настоящее время при современном развитии технологий [6. С. 102].

Таким образом, подводя итог вышеизложенному, необходимо констатировать, что возможности использования систем цифровизации и систем искусственного интеллекта в уголовно-процессуальной деятельности многообразны и вариативны. Цифровизация правотворческой и правоприменительной системы нашего государства это только вопрос времени.

Список литературы

1. Ахмеджанова Р. Р. Может ли искусственный интеллект заменить человека-судью? // Юриспруденция 2.0: новый взгляд на право: Материалы межвузовской научно-практической конференции с международным участием (г. Москва, 8 декабря 2017 г.): Сборник научных статей. Москва: Российский университет дружбы народов. 2017. С. 461–466; Брановицкий К. Л. Соотношение понятий «качество» и «цифровизация правосудия» // Арбитражный и гражданский процесс. 2019. № 7. С. 3–7;

Заплатина Т. С. Искусственный интеллект в вопросе вынесения судебных решений, или ИИ-судья // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 4 (56). С. 160–168; Морхат П. М. Применение искусственного интеллекта в судебном процессе // Вестник гражданского процесса. 2019. Т. 9, № 3. С. 61–85; Незнамов А. В. К вопросу о применении технологий искусственного интеллекта в правосудии: терминологический аспект // Арбитражный и гражданский процесс. 2019. № 10. С. 14–18.

2. Бурлака С. Н. Цифровизация правотворчества: тенденции развития // Взаимодействие власти, бизнеса и общества в правотворческой деятельности. Материалы XIII Международной научно-практической конференции. 2020. С. 43–47; Кич И. С. Переосмысление понятия «правотворчество» в условиях цифровизации экономики и права // Юридический вестник Кубанского государственного университета. 2020. № 4. С. 14–17; Куракина С. И., Круглов Д. Н. О перспективах цифрового правотворчества // Гуманитарные, социально-экономические и общественные науки. 2019. № 10. С. 168–171; Пашенцев Д. А. Правотворчество в условиях развития современных цифровых технологий // Российская правовая система в условиях четвертой промышленной революции. Материалы VI Московского юридического форума XVI Международной научно-практической конференции. В 3 частях. 2019. С. 331–333.

3. Гриффин Эндрю. Роботы-судьи скоро смогут помогать в судебных делах. 24 октября 2016. URL: https://www.independent.co.uk/life-style/gadgets-and-tech/news/ai-judge-robot-european-court-of-human-rights-law-verdicts-artificial-intelligence-a7377351.html (дата обращения: 29.08.2022).

4. Зенин С. С., Кутейников Д. Л., Ижаев О. А., Япрынцев И. М. Технология блокчейн в правотворчестве: опыт применения // Проблемы права. 2020. № 2 (76). С. 46–50; Зенин С. С., Кутейников Д. Л., Ижаев О. А., Япрынцев И. М. Правотворчество в условиях алгоритмизации права // Lex russica. 2020. Том 73. № 7 (164). С. 23–27.

5. Исенеков С. А. В Китае создали «нейропрокурора» для типичных уголовных дел – он выдвигает обвинения с точностью 97 %. URL: https://tjournal.ru/tech/501066-v-kitae-sozdali-neyroprokurora-dlya-tipichnyh-ugolovnyh-del-on-vydvigaet-obvineniya-s-tochnostyu-97 (дата обращения: 05.02.2022); Марина С. А. В Китае разработали цифрового прокурора. 27 декабря 2021 г. URL: https://lenta.ru/news/2021/12/27/ai_prosecutor// (дата обращения: 29.08.2022).

6. Карпов В. Э., Готовцев П. М., Ройзензон Г. В. К вопросу об этике и системах искусственного интеллекта // Философия и общество. – 2018. – № 2. – С. 102.

7. Ладыгина И. В. Социально-этические проблемы робототехники // Вестник Вятского государственного университета. 2017. № 3. С. 27–31; Разин А. В. Этика искусственного интеллекта // Философия и общество. 2019. № 1. С. 57–73.

8. Мариссаль Пьеррик. Реформа Беллубе. Программное обеспечение вместо судей, Мираж прогностического правосудия. 20 апреля 2018 г. URL: https://www.humanite.fr/reforme-belloubet-des-logiciels-la-place-des-juges-mirage-de-la-justice-predictive-654139 (дата обращения: 29.08.2022).

9. Николаос Алетрас, Димитриос Царапацанис, Даниил Преотиук-Пьетро, Василейос Лампос. Прогнозирование судебных решений Европейского Суда по правам человека: перспектива обработки естественного языка 24 октября 2016 г. URL: https://peerj.com/articles/cs-93/// (дата обращения: 29.08.2022).

10. Остроумов Н. В. Искусственный интеллект в праве: обзор существующих концепций правового регулирования отношений с участием носителей искусственного интеллекта // Законность и правопорядок. 2021. № 3 (31). С. 61–66.

11. Приказ Генерального прокурора Республики Казахстан от 03.01.2018 № 2 «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате» (с изменениями от 15.02.2021 г.). URL: https://online.zakon.kz/document/?doc_id=34195283&pos=5;-108#pos=5;-108 (дата обращения: 29.08.2022).

12. Синкевич В. В. Цифровизация уголовного процесса: зарубежный и отечественный опыт // Вестник Волгоградской академии МВД России. 2022. № 1(60). – С. 133.

13. Тормасов В. А. Автоматизация, информационные технологии, цифровые технологии – в чем разница? URL: https://решение-верное.рф/digital-transformation-fast (дата обращения: 29.08.2022).

14. Уголовно-процессуальный кодекс Республики Казахстан от 04.07.2014 № 231-V (с изменениями и дополнениями по состоянию на 03.09.2022 г.). URL: https://online.zakon.kz/document/?doc_id=31575852&doc_id2=31575852#pos=53;-83&pos2=1213;-82 (дата обращения: 29.08.2022).

15. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н. А. Голованова, А. А. Гравина, О. А. Зайцев и др.; Ин-т законодательства и сравн. Правоведения при Правительстве РФ. Москва: Контракт, 2019. С. 120.

16. Фоков А. П. Концепция развития электронного правосудия в российской федерации: настоящее и будущее // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2021. № 7. С. 132; Шестернина Д. С. Вопросы реализации стандартов правосудия в условиях применения электронной процессуальной формы и развития системы «электронного правосудия» // Научный электронный журнал Меридиан. 2020. № 4 (38). С. 147; Яровая М. В. Электронное правосудие: зарубежный опыт применения // Право и права человека в современном мире: тенденции, риски, перспективы развития. Материалы Всероссийской научной конференции, посвященной памяти профессора Ф. М. Рудинского. Под общей редакцией В. В. Строева, Д. А. Пашенцева, Н. М. Ладнушкиной. Москва, 2021. С. 192.

17. Хатсон Метью. Искусственный интеллект преобладает при прогнозировании решений Верховного суда. 2 мая 2017 г. URL: https://www.science.org/content/article/artificial-intelligence-prevails-predicting-supreme-court-decisions (дата обращения: 29.08.2022).

18. Цифровизация и ее место в современном мире 5 июля 2021 г. URL: https://www.gd.ru/articles/10334-tsifrovizatsiya (дата обращения: 29.08.2022).

19. Чен Стивен. Китайские ученые разрабатывают ИИ – «обвинителя», который может выдвигать свои собственные обвинения. 26 декабря 2021 г. URL: https://www.scmp.com/news/china/science/article/3160997/chinese-scientists-develop-ai-prosecutor-can-press-its-own?module=perpetual_scroll_0&pgtype=article&campaign=3160997 (дата обращения: 29.08.2022).

А. А. Ходусов,
кандидат юридических наук, доцент,
Международный юридический институт

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ ЗАКОНОДАТЕЛЬСТВА ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

Аннотация. В данной работе проведен анализ проблем и путей совершенствования законодательства об уголовной ответственности за совершение преступлений в сфере обращения цифровой информации. Проведен анализ статьи 272 УК РФ – неправомерный доступ к компьютерной информации, ее объект и предмет, судебная практика и ее основные проблемы в системе уголовного права, также автор рассмотрит вопросы квалификации данного преступления в зарубежной практике.

Ключевые слова: Уголовный кодекс РФ, компьютерная информация, квалификация, проблемы, обращение цифровой информации

ON THE ISSUE OF IMPROVING THE LEGISLATION ON CRIMINAL LIABILITY FOR CRIMES IN THE FIELD OF DIGITAL INFORMATION CIRCULATION

Abstract. This paper analyzes the problems and ways to improve the legislation on criminal liability for crimes in the field of digital information circulation. The analysis of Article 272 of the Criminal Code of the Russian Federation – illegal access to computer information, its object and subject, judicial practice and its main problems in the criminal law system, the author will also consider the issues of qualification of this crime in foreign practice.

Keywords: Criminal Code of the Russian Federation, Computer information, Qualification, Problems, Circulation of digital information

С развитием технологий, возможности человека, у которого есть персональный компьютер, становятся гигантскими, начиная от покупки вещей в сети Интернет и заканчивая ведением бизнеса через интернет.

При этом человек так же, как и в обычном пространстве подвергается постоянной опасности совершения в отношении его преступного посягательства, а именно, у него в любой момент могут завладеть личной информацией, которая хранится в компьютере. В связи с этим необходимо разобрать актуальные проблемы уголовного законодательства относительно данной статьи, что может послужить улучшению методов борьбы с злоумышленниками, пытающимися завладеть чужой компьютерной информацией [4].

Следующие составы, по мнению МВД России, относятся к уголовным делам в сфере информационных технологий следующие составы преступлений: ст. 158, 159, 159.3, 159.6 УК РФ (кражи и мошенничества при использовании технологий в сфере компьютерной информации), 171.2, 205.2, 228.1 242, 242.1, 242.2, 280 УК РФ; преступления в сфере компьютерной информации, предусмотренные главой 28 УК РФ (ст. 272–274.1 УК РФ).

По мнению некоторых авторов, преступления в сфере компьютерной информации не ограничиваются главой 28 УК РФ, к данной категории возможно отнести любое преступление, совершенное с использованием телекоммуникационных и компьютерных технологий, в частности преступления в кредитно-финансовой деятельности (преступная банковская деятельность, отмывание и т. п.).

При установлении понятия категории преступлений необходимо установить такие понятия, как «информационно-телекоммуникационные технологии» и «компьютерная информация».

Первым этапом в процессе доказывания является установление факта совершения преступления.

Установление факта совершения преступления необходимо при принятии решении о возбуждении уголовного дела, если не установлен факт совершения преступления, то нет оснований для возбуждения дела.

Выделяют способы совершения преступлений в сфере информационных технологий: способ непосредственного воздействия на компьютерную и иную информацию; способ опосредованного (удаленного) воздействия на компьютерную информацию: удаленное проникновение в информационно-телекоммуникационные сети [5].

В ходе анализа положений УПК РФ ст. 64 Закона № 126-ФЗ установлено, что законодательство РФ не устанавливает понятие лог-файлов, не регулирует отдельно порядок их предоставления следователю. Следователь таких прав не имеет, поскольку он собирает доказательства в рамках следственных действий. Согласно ч. 5 ст. 64 Закона № 126-ФЗ операторы не передают информацию следователю, а оказывают содействие в рамках следственных действий. В связи с этим возникает проблема, такого следственного действия как получение компьютерной информации не существует, а действующие следственные действия не позволяют получать информацию с технических каналов связи в ходе доследственной проверки.

При доказывании необходимо устанавливать и иные обстоятельства, указанные в ст. 73 УПК РФ. На основе анализа процессуальных действий, проводимых в ходе проверки сообщения о преступлении, установлено, что Конституционный суд Российской Федерации в Определении от 22.12.2015 № 2885-О установил, что истребование документов возможно в рамках досудебной проверки, только при наличии согласия на их передачу.

В данной ситуации необходимо установить, что истребование должно осуществляться на основании ч. 4 ст. 21 УПК РФ. Истребование документов необходимо для целей возбуждения уголовного дела в проведения обыска у подозреваемого. Тактика субъекта доказывания не должна быть направлена на раскрытие информации о проверке сообщения о преступлении, поскольку, если преступник узнает, что в отношении него проводится проверка, он попытается уничтожить следы.

В ходе анализа ст. 145.1 УПК РФ сделан вывод, что необходимо обязательно изымать электронные носители по делам в сфере информационных технологий, что следует из анализа ст. 145.1 УПК РФ, за исключением ограничений, установленных статьей.

Статьи УК РФ иногда сгруппированы таким образом, что дают некоторым толкователям возможность подменять значение признаков состава преступления

и придавать слишком большое значение информации, относя ее к предмету посягательства, например, в преступлениях, предусмотренных ст. 325 и ст. 327 УК РФ.

Документы (даже официальные) не представляют социальной ценности сами по себе, но важны, потому что содержат юридически значимые факты или статусы, которые удостоверяют. Причем ценность указанных предметов проявляется только в возможности их использования в свою пользу или против чужих интересов [3].

Документ – лишь материальный носитель этой знаковой информации. Реальная общественная опасность незаконных манипуляций с ними возникает именно тогда, когда этой информацией, зафиксированной документально, начинают пользоваться вопреки правилам и причиняют вред. До этого момента нет воздействия на конкретный вид социально-значимого блага, которое бы могло олицетворять объект преступления.

Примером аналогичного заблуждения относительно места признака в системе состава преступления могут служить объекты интеллектуальной собственности. Настоящую социальную (а не персонифицированную в авторском праве ценность) они обретают только на уровне предметов, участвующих в экономическом обороте (ст. 146 и ст. 147 УК РФ предполагают наступление имущественного ущерба для правообладателей). То есть незаконное использование экономически невостребованного объекта интеллектуальной собственности не может создать общественно опасного деяния. Деяния, запрещенные некоторыми статьями УК РФ, посвященными «нарушению специальных правил» (например, в сфере экологии), иногда тоже относятся в юридической литературе к преступлениям, где предметом выступают сами эти правила [6].

В такой «транскрипции», когда признак предмета преступления выходит за рамки классической концепции: вещи материального мира, воздействуя на которые виновный причиняет вред объекту уголовно-правовой охраны», он смешивается с категорией средств совершения преступления.

Именно в этот момент во многих составах преступлений, закрепленных в уголовном законе, происходит преувеличение значения информации – вместо средства ее начинают считать самоцелью посягательства. Нарушение правил оборота государственной тайны причиняет вред не этому обороту, а общественным отношениям по поводу государственной безопасности. Разглашение тайны усыновления нарушает личные границы, и вред причиняется личности, а не обороту актов гражданского состояния. Исключением может служить, пожалуй, информация, предоставляемая в процессе судопроизводства и предварительного следствия.

Так как правосудие основано на поиске истины, которая может выявляться только при условии достоверности данных, то любое искажение информации влияет на итог, а значит на объект уголовно-правовой охраны. Искажение данных в официальных документах в результате приведет к нарушению отдельных видов прав субъектов общественных отношений в какой-либо сфере жизни (экономической, семейной, трудовой или др.). В этом случае следовало бы квалифицировать содеянное, исходя из вида пострадавшего объекта.

Аналогичная ситуация прослеживается при ближайшем рассмотрении посягательств, предусмотренных ст. 272–274.1 УК РФ. Компьютерная (цифровая) ин-

формация – это не столько вид информации (она может относиться к любой сфере жизнедеятельности социума и его участников), сколько форма ее существования. Подход, согласно которому глава 28 не должна выделяться в УК РФ в качестве самостоятельной, так как не имеет собственного объекта уголовно-правовой охраны, также присутствует в теории отечественного уголовного права.

В силу специфики (исключительно физической) хранения и передачи такой информации, реальная опасность ее утраты ничем не отличается от утраты сведений на других, не компьютеризированных носителях. Сам факт существования цифровых данных не делает из них иные сведения, и отличие от любой другой информации заключается здесь только в способе фиксации и хранения, т. е. в форме. Сложившаяся тенденция по усилению уголовной ответственности за совершение преступлений (в частности, вербальных) посредством информационно-коммуникационных сетей в ст. 110.2, 137, 205.2, 230, 280, 280.1 УК РФ, на наш взгляд, преувеличивает объемы необходимой репрессии за использование цифровой среды и цифровой информации в рамках криминального поведения.

Несанкционированное копирование компьютерной информации, криминализированное ст. 272 УК РФ, например, явно не охватывает такие способы тиражирования, как фотографирование экрана или переписывание вручную сведений [5. С. 529].

Хотя в зависимости от последствий, выделенные способы все равно могут нарушать тайну переписки или даже государственную тайну, быть приготовлением или покушением к иным видам преступлений, т. е. обладать общественной опасностью в рамках традиционных объектов посягательств.

Вопрос о нарушениях и злоупотреблениях компьютерной информацией, относящейся к программному обеспечению (например, вредоносные программы), на наш взгляд, может также решаться через призму причиненного вреда правообладателям легального контента. Распространенные в настоящее время «компьютерное хулиганство», «компьютерное мошенничество» и др. т. п. деяния вполне можно квалифицировать по имеющимся в УК РФ статьям вне пределов главы 28, если признать, что компьютерная (цифровая) информация – не само ценность, а форма существования сведений.

Иными словами, считаем, что выделять самостоятельный объект уголовно-правовой охраны в виде отношений по поводу оборота компьютерной информации – неоправданное расширение уголовной репрессии.

Важно определить объект и предмет ст. 272 УК РФ. Некоторые авторы считают, что у нормы статьи, объект и предмет тождественны, однако, как пишет законодатель, предмет не находится в ограниченной связи с объектом данного преступления [1].

Как и в большинстве норм уголовного кодекса, связанных с имуществом, объектом данного преступления принято считать не завладения определенной компьютерной информацией, а общественные отношения, которые обеспечивают конфиденциальность и сохранность компьютерной информации.

Предметом же будет являться охраняемая законом компьютерная информация.

Таким образом, можно заметить, что объект отвечает за конкретные действия, направленные на законное хранение и оборот информации, хранящейся на компьютере [2].

На сегодняшний день проблема возбуждений уголовных дел по ст. 272 УК РФ является неоднозначной.

Интернет не ограничивается одним городом или страной, он связан со всем миром, в этом же и проявляется немаловажная проблема, она заключается в том, что если похищение злоумышленником данных происходит в конкретной стране и в конкретном городе, то это возможно пресечь, однако, если хищение данных исходит из других стран, то тут уже не физически не юридически невозможно воздействовать на злоумышленника. Единственное, что необходимо в данном случае это обезопасить информацию, хранящуюся на компьютере при помощи различных антивирусных программ и не скачивать подозрительные программы, которые могут поспособствовать хищению данных [5].

Существует проблема и квалифицирующего характера, она связана с тем, что преступным деянием является именно неправомерный доступ к информации, которая содержится на компьютере, а не на каком-либо носителе данной информации. В этом случае такое деяние может быть квалифицированно как умышленное уничтожение или повреждение имущества (ст. 167 УК РФ).

Проблема заключается в том, что при уничтожении носителя данной информации санкция предусмотрена более мягкая мера наказания, чем в ст. 272 УК РФ.

Также существует проблема доказательства удаления ценной информации, это необходимо для квалификации ч. 2 ст. 272 УК РФ (причинившее крупный ущерб), ведь уничтожение компьютерной информации предполагает ее исчезновение без возможности восстановления, что может повлечь затруднения в уголовном процессе.

Важной деталью является то, что законодатель делает акцент на тех сведениях, по которым неправомерный доступ может причинить огромный ущерб, законодательство Российской Федерации выделяет следующие сведения:

– Тайна следствия и судопроизводства.

– Факты и события частной жизни гражданина, идентифицирующие его личность.

– Служебные сведения (в соответствии с ГК).

– Тайна профессиональной деятельности (пример: адвокатская тайна).

– Тайна коммерческой деятельности.

– Интеллектуальная тайна (пример: еще неопубликованные изобретения).

Рассмотрев данные сведения, важно заметить, что законодатель понимает уязвимые стороны различных областей страны, однако, как и говорилось ранее, методы предотвращения хищений данных сведений через электронные системы слабо развиты, именно поэтому, когда во всем мире происходит процесс переноса данных на виртуальные носители, государству также необходимо задуматься о надежной защите этих данных, не только посредством введения уголовно наказуемых норм в Уголовный кодекс РФ, но и разработкой методов предотвращения данных преступлений.

На данный момент ситуация со ст. 272 УК РФ не однозначна. С одной стороны, наше законодательство не только дает понимание о противоправности деяний, связанных с неправомерным завладением информацией, но и в отличие от законодательств других стран разделяет по способу ее совершения [6].

С другой стороны, до конца непонятна сама необходимость данного разделение, ведь оно может порождать проблемы в правоохранительной системе, что и наблюдается на сегодняшний день.

Наконец нужно отметить, что российскому законодательству в данном вопросе еще предстоит множество изменений и дополнений, прежде всего уже на сегодняшнем этапе необходимо выделить наиболее действенные методы противодействия незаконному получению компьютерной информации, а также необходимо повышать квалификацию правоохранительных органов в сфере компьютерной безопасности, хотя как вариант можно использовать привлечение специалистов для разработки более действенных программ, отслеживающих следы компьютерных преступлений [3. С. 60].

Таким образом, повышение интереса правоохранительных органов к компьютерной безопасности сделает отличную базу для безопасного перехода Российской Федерации к информационному прогрессу.

Ознакомившись с архивами судебных решений за исследуемый период, можно сделать следующие выводы, что по ст. 273 УК РФ в настоящий момент существует множество неоднозначных вопросов по проблеме применения рассматриваемой статьи, споры о правильном решении которых, в научной среде ведется до сих пор.

Получение информации, путем хищения с электронного носителя, на законодательном уровне называется мошенничеством и его классическое понятие имело закрепление в ст. 159 УК РФ. Но в ходе изменений УК РФ, рассматриваемый нами объект посягательства, получил свое закрепление в ст. 159.6 УК РФ «мошенничество в сфере компьютерной информации», что и будет исследовано нами далее.

В ней рассматривается мошенничество, т. е. хищение чужого имущества путем кражи электронного носителя, но виды мошенничества очень разнообразны, даже в сфере IT-технологий вариантов совершения подобных преступлений очень много [7].

Неоднократно А. А. Чугунов утверждал, что: «мошенничество предполагает наличие потерпевшего, которого можно обмануть или чьим доверием можно злоупотребить, что является ключевым фактором для отнесения общественно опасного деяния к данному виду преступления».

С подобным высказыванием невозможно не согласиться, но получается, что ст. 159.6 УК РФ не имеет весь спектр, относящийся к мошенничеству, именно если оно касается IT-технологий, ведь в большинстве случаев потерпевшие даже не подозревают о наличии злоумышленника в их электронном носителе. В любом случае на техническое средство невозможно воздействовать как на человека, с точки зрения эмоций, чувств или же путем злоупотребления доверия. Из этого следует, что данная статья в УК РФ не совсем точно определяет объективную сторону состава рассматриваемого преступления. На наш взгляд, было бы более правильно откорректировать объективные признаки состава преступления в сфере мошенничества.

Если же для мошенника основной целью является хищение денежных средств или информации, путем подбора паролей, входа с чужой учетной записи или подбора пин-кода, то в подобной ситуации правильнее утверждать о тайном хищении чужой информации или имущества, путем использования компьютерных технологий.

Так в своей статье А. Н. Харитонов и Е. В. Никульченкова утверждают, что: «одним из путей решения данной проблемы видится исключение ст. 159.6 УК РФ из уголовного закона с последующим внесением изменения в виде квалифицирующего признака в ст. 158 УК РФ: кража, совершенная с использованием компьютерных технологий».

Таким образом, мнения по рассматриваемой проблеме поделились, некоторые считают, что правильнее будет проработать ст. 159.6 УК РФ, а другие придерживаются мнения исключения подобной статьи из УК РФ и внесения данных объективных признаков в ст. 158 УК РФ в качестве квалифицирующего признака.

В любом случае по опыту применения данной статьи можно сделать вывод, что она является до конца не проработанной, а, значит, в судебно-следственной практике будет иметься большое количество недочетов и ошибок.

В них говорится о сознательном уничтожении информации, блокировке, копировании данных, хранении, передаче данных, при помощи вирусных программ, программ-шпионов или иных вредоносных систем. Даже в случае, если преступнику в сфере компьютерной информации не удастся до конца заполучить данными или применить их в своих корыстных целях, он все равно будет привлечен к уголовной ответственности, так как перечисленные составы имеют вид формальных.

Примером может послужить дело, в котором гражданин В., самостоятельно разработал вирусную программу – спам для получения личной информации законопослушных граждан через социальные сети.

После того как люди стали переходить по его ссылке, заранее отправленной в социальной сети, часть информации, а зачастую и логины с паролями переходили на личный компьютер гражданина В. В последующем он был привлечен к уголовной ответственности по ст. 273 УК РФ [8].

Таким образом, преступник, применивший в отношении законопослушного гражданина неправомерное деяние, будет нести ответственность за любой вред, причиненный с его стороны, но ответственность по статье «Мошенничество в сфере компьютерной информации» не наступит в связи с тем, что сам носитель информации будет находиться у потерпевшего.

На наш взгляд, глава 28 УК РФ достаточно подробно описывает компьютерные преступления. Однако в ней не рассматривается специфика мошенничества в целом, а значит, эта глава также может быть существенно изменена.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25 ст. 2954 (в ред. 14.07.2022). URL: https://normativ.kontur.ru/document?moduleId=1&documentId=427835 (дата обращения: 19.08.2022).

2. Абов А. И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации. URL: https://search.rsl.ru/ru/record/01002559391 (дата обращения: 19.08.2022)

3. Анисимова И. А. Уголовно-правовое значение преступного вреда: Дисс. … канд. юрид. наук. Томск, 2008. 232 с.

4. Бражник С. Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дисс. … канд. юрид. наук. Ижевск. 2002. 189 с.

5. Евдокимов К. Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области). URL: https://cyberleninka.ru/article/n/osobennosti-lichnosti-prestupnika-sovershayuschego-nepravomernyy-dostup-k-kompyuternoy-informatsii-na-primere-irkutskoy-oblasti (дата обращения: 19.08.2022).

6. Пелевина А. В. Криминообразующие признаки диспозиции статьи 272 УК РФ // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 4 (32). С. 261–267.

7. Старичков М. В. Понятие «Компьютерная информация» в российском уголовном праве. URL: https://www.elibrary.ru/item.asp?id=21342806 (дата обращения: 19.08.2022).

8. Табаков А. В. Уголовное наказание за неправомерный доступ к охраняемой законом компьютерной информации: толкование текста статьи 272 УК РФ и обоснование необходимости внесения в нее изменений. URL: https://cyberleninka.ru/article/n/ugolovnoe-nakazanie-za-nepravomernyy-dostup-k-ohranyaemoy-zakonom-kompyuternoy-informatsii-tolkovanie-teksta-stati-272-uk-rf-i (дата обращения: 19.08.2022).

Е. А. Черкасова,
кандидат юридических наук,
Белгородский государственный национальный
исследовательский университет

ЦИФРОВЫЕ ТЕХНОЛОГИИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

Аннотация. Целью статьи является исследование современного состояния применения цифровых технологий в уголовном процессе, а также перспектив перехода к электронному уголовному судопроизводству. В статье исследованы позиции ряда ученых-процессуалистов о перспективах расширения информационных технологий в уголовном процессе. Высказана точка зрения об основных этапах перехода к новым цифровым технологиям в уголовном судопроизводстве.

Ключевые слова: уголовно-процессуальное законодательство, цифровизация, цифровые технологии, электронное уголовное дело, электронные документы, электронные носители информации, электронное производство по уголовным делам

DIGITAL TECHNOLOGIES IN CRIMINAL PROCEEDINGS: CURRENT STATUS AND PERSPECTIVES

Abstract. The purpose of this article is to study the current state of the use of digital technologies in criminal proceedings, as well as the prospects for the transition to electronic criminal justice. The article examines the positions of a number of procedural scientists on the introduction of information technology in the criminal process. A point

of view was expressed on the main stages of the transition to new digital technologies in criminal proceedings.

Keywords: Criminal procedure legislation, Digitalization, Digital technologies, Electronic criminal case, Electronic documents, Electronic storage media, Electronic criminal proceedings

Современный мир невозможно представить без постоянно развивающихся и все более внедряющихся в нашу жизнь цифровых технологий передачи и обработки информации. Информационно-коммуникационные технологии применяются в различных сферах взаимодействия общества и государства, однако назвать их применение равномерным нельзя. Так, уголовное судопроизводство можно отнести к видам государственной деятельности, в наименьшей степени подвергшимся цифровизации.

Как справедливо отмечает Л. А. Воскобитова, «нельзя не признать, что в российском уголовном судопроизводстве пока это лишь отдельные, робкие «вкрапления» цифровых технологий в сложную, конфликтную, противоречивую, многофакторную процессуальную деятельность, осуществляемую преимущественно человеком» [2. С. 91].

Современное уголовно-процессуальное законодательство, а также связанные с ним подзаконные нормативные акты регламентируют применение ряда цифровых технологий, касающихся как собирания доказательств, так и организации производства по уголовному делу.

Так, на стадии возбуждения уголовного дела допускается возможность приема заявлений о преступлениях в электронной форме, направляемых посредством официальных сайтов. Такая форма приема сведений значительно облегчает усилия лиц, получивших информацию о преступлении, по передаче сведений в компетентный правоохранительный орган.

Применение при производстве ряда следственных действий аудио- и видеозаписи является дополнительным средством фиксации их процедуры и результатов, а также позволяет следователю не привлекать к участию в них понятых. Доказательственное значение имеют результаты контроля и записи телефонных и иных переговоров, сведения, содержащиеся в электронных сообщениях. Получить показания в ходе допроса, очной ставки и опознания можно с помощью использования систем видеоконференцсвязи, облегчающих и ускоряющих процедуру получения доказательств. Регламентирован порядок изъятия электронных носителей информации и копирования с них информации в ходе следственных действий. Материалы аудио- и видеозаписи могут получить статус доказательств по уголовному делу, что важно в современных условиях электронного видеонаблюдения в магазинах, учреждениях, на улицах городов.

Для судебного производства по уголовному делу характерны элементы цифровизации. Ведение аудиопротоколирования при рассмотрении уголовного дела в открытом судебном заседании судом первой и апелляционной инстанции позволяет в дальнейшем ознакомиться с аудиозаписью судебного заседания заинтересованным участникам уголовного судопроизводства и вышестоящему суду. Проведение

допроса свидетеля в судебном заседании с помощью систем видеоконференц-связи экономит судебные расходы на его прибытие в суд. Сообщение потерпевшим суду адреса электронной почты способствует быстрому направлению информации о местонахождении и освобождении осужденного.

С 2016 г. закон позволяет использовать ряд электронных документов в уголовном судопроизводстве. Так, ходатайства, жалобы, заявления, представления заинтересованные лица могут подавать в суд в форме электронного документа, подписанного электронной подписью. Копия судебного решения в электронном виде может направляться участнику уголовного процесса с помощью сети Интернет.

Кроме того, значительно облегчили работу юристам, в том числе, участвующим в производстве по уголовному делу, справочно-правовые системы («Гарант», «КонсультантПлюс», и другие), позволяющие быстро найти необходимую правовую информацию. Благодаря созданию государственной автоматизированной системы «Правосудие» база судебных решений, выносимых по уголовным делам, стала открытой и доступной.

Несмотря на появление отдельных элементов цифровизации в уголовном судопроизводстве, следует согласиться с П. П. Ищенко, что «закрепленные в законе отдельные процедуры, допускающие использование цифровых технологий, не образуют завершенной системы, которая позволила бы перейти к полностью электронному производству по уголовным делам» [3. С. 69].

Российскими учеными-процессуалистами в последние годы все чаще поднимается вопрос о возможности перехода к электронному уголовному делу.

Так, по мнению О. В. Качаловой, «наиболее приемлемым вариантом внедрения современных информационных технологий в уголовное судопроизводство представляется последовательное изменение уголовно-процессуального закона и внедрение электронных технологий на организационном уровне с целью адаптации производства по уголовным делам к цифровой реальности, результатом которой станет переход к электронному уголовному делу либо отдельным его элементам» [4. С. 95–96].

Т. Ю. Вилкова и Л. Н. Масленникова полагают, что «развитие цифровых технологий и совершенствование законодательного регулирования использования электронного уголовного дела должно привести к оптимизации взаимодействия государственных органов и лиц, заинтересованных в доступе к правосудию, повысить доверие граждан к деятельности государственных органов, установить дополнительные гарантии принципов законности в уголовном судопроизводстве» [1. С. 730].

На наш взгляд, внедрение цифровых технологий в уголовное судопроизводство и переход к электронному уголовному делу неизбежны. Однако этот процесс должен быть поэтапным, последовательным и тщательно разработанным. Он должен опираться на внимательное изучение передового опыта зарубежных государств, подготовку нормативно-правовой основы в виде принятия нового уголовно-процессуального законодательства, разработку необходимого программного обеспечения, повышение квалификации в области цифровых технологий участниками уголовного процесса, ведущими производство по уголовному делу. Необходимым условием перехода к новым цифровым технологиям в уголовном судопроизводстве должно быть соблюдение прав его участников.

Список литературы

1. Вилкова Т. Ю., Масленникова Л. Н. Законность и унификация в уголовном судопроизводстве: от бланков процессуальных документов – к электронному уголовному делу // Вестник Пермского университета. Юридические науки. 2019. Вып. 46. С. 728–751.

2. Воскобитова Л. А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex Russica. 2019. № 5 (150). URL: https://cyberleninka.ru/article/n/ugolovnoe-sudoproizvodstvo-i-tsifrovye-tehnologii-problemy-sovmestimosti (дата обращения: 16.09.2022).

3. Ищенко П. П. Современные подходы к цифровизации досудебного производства по уголовным делам // Lex Russica. 2019. № 12 (157). URL: https://cyberleninka.ru/article/n/sovremennye-podhody-k-tsifrovizatsii-dosudebnogo-proizvodstva-po-ugolovnym-delam (дата обращения: 16.09.2022).

4. Качалова О. В. Уголовно-процессуальные проблемы информатизации современного уголовного судопроизводства // Российское правосудие. 2019. № 2. С. 95–98.

А. А. Черноперов,
старший преподаватель,
Санкт-Петербургская академия
Следственного комитета Российской Федерации

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ СЛЕДОВ В ДОКАЗЫВАНИИ

Аннотация. Статья посвящена определению нового понятия «цифровой след» в криминалистике. Автором с практической точки зрения оценивается значение поиска, выявления, фиксации, изъятия и исследования следов, возникающих при взаимодействии цифровых систем, обосновывается необходимость введения нового термина и приводится одна из формулировок термина «цифровой след». В статье приведены анализ значения использования цифровых следов в доказывании по уголовным делам, способы определения владельца информации и носителей информации, а также способы объективации процесса доказывания через визуализацию цифровых данных.

Ключевые слова: цифровая криминалистика, цифровой след, цифровая информация, электронный носитель информации, владелец информации, объективация доказывания, визуализация

THE USE OF DIGITAL TRACES IN THE INVESTIGATION

Abstract. The article is devoted to the definition of a new concept of “digital footprint” in criminology. From a practical point of view, the author evaluates the importance of searching, identifying, fixing, removing and investigating traces arising from the interaction of digital systems, justifies the need to introduce a new term and provides one of the formulations of the term “digital footprint”. The article provides an analysis of the importance of using digital traces in proving criminal cases, ways to

determine the owner of information and information carriers, as well as ways to objectify the proof process through the visualization of digital data.

Keywords: Digital forensics, Digital footprint, Digital information, Electronic media, Owner of information, Objectification of evidence, Visualization

В соответствии с данными статистики, которые приводит в своей статье Председатель Следственного комитета Российской Федерации А. И. Бастрыкин, «…в 2019 году выявлено 8 812 таких преступлений, в 2020–11493 (+30,4 %), в 2021–12112 (+5,4 %). При этом качество проводимых Следственным комитетом расследований находится на стабильно высоком уровне, а общий объем раскрытых и расследованных преступлений в сфере ИКТ растет пропорционально повышению числа зарегистрированных правонарушений» [1. С. 4]. При расследовании указанной категории преступлений правоприменители сталкиваются с отсутствием единого определения новых явлений, происходящих в сфере информационно-коммуникационных технологий, необходимостью разработки новых методик производства следственных действий при расследовании преступлений указанной категории.

Сразу же необходимо оговориться, что, как и в любой другой недавно возникшей и активно развивающейся отрасли, в информационных технологиях происходит формирование терминологического аппарата и можно встретить разные определения одних и тех же явлений и процессов. Например, понятие «цифровой след» в криминалистике и информационной безопасности имеет абсолютно разные, не связанные значения.

В информационной безопасности значение этого термина узкое и связано только со злонамеренными действиями во время компьютерных инцидентов. В криминалистике же значение этого термина намного шире и включает в себя (об этом мы поговорим позже) все виды взаимодействия. То же можно сказать и о значении терминов в программировании, разработке сценариев и алгоритмов. Поэтому, чтобы избежать неопределенности и ошибочных выводов, договоримся, что в рамках данной статьи будет использоваться только криминалистическим значением терминов.

Итак, что же такое «цифровой след»? «След» является ключевым понятием криминалистики. Первые попытки поиска преступников предпринимались нашими предками как раз через поиск следов. Первыми «криминалистами» были охотники-звероловы, которые из поколения в поколение передавали навыки поиска следов животных и определения по ним давности образования следов, направления движения, размеров зверя и другой информации, важной для удачной охоты. Именно следопыты искали воров и убийц по их следам. Корень «след» содержат такие слова как «следователь», «исследовать» и другие.

В науке криминалистики след является системообразующим понятием, на основе которого строится ее понятийный аппарат и терминология.

Чем дальше развивается наука, тем больше видов следов появляется в криминалистике. Если в конце XIX в. интерес для криминалистов представлял только рисунок папиллярных узоров в следе руки, то в конце XX в. этот след изучался уже не только как рисунок, но и как носитель уникальной информации на молекулярном уровне.

С позиций теории отражения подготовка, совершение и сокрытие любого преступления, в том числе и компьютерного, как и любое другое событие в материальном

мире, всегда вызывает изменения в окружающей среде. Такие изменения и являются следами. Следы возникают всегда, когда происходит взаимодействие двух и более объектов. Что касается взаимодействия физического, то следы такого взаимодействия очевидны и бесследно оно не проходит. При этом объект, который оставляет следы (отражаемый), например, монтировка, использованная для взлома, называют следообразующим. Второй же объект (отражающий), несет на себе как информацию об отражаемом объекте (размеры, форма окончания), так и информацию о способе взаимодействия (удары или давление). Второй объект называют следовоспринимающим.

Следует помнить, что отражаемый объект выступает в то же время и отражающим (частицы краски от косяка на монтировке, кровь потерпевшего на ноже и так далее).

В информационной среде взаимодействие происходит между двумя и более устройствами, результатом которого является изменение информации, хранящейся на каждом из них. Причем, у следов взаимодействия в информационной среде также есть материальная форма, которая выражается в физических устройствах, на которой постоянно или временно хранится изменяемая информация.

Следы, образовавшиеся в результате взаимодействия электронных устройств, наравне со следами взаимодействия преступника с элементами устройства и вещной обстановки места происшествия относятся к объективным следам и должны быть выявлены, изъяты, подвергнуты экспертному исследованию и использованы в доказывании наряду с субъективными доказательствами (показания потерпевшего, свидетелей, иных лиц).

При этом особенности формирования и сохранения следов в электронной среде выделяют их из всей массы криминалистически значимых следов, что потребовало их выделения в отдельный класс – цифровых следов.

Одним из авторов и редактором первого в нашей стране учебника по цифровой криминалистике В. Б. Веховым дается следующее определение указанной группы следов. «Цифровой след – это любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (прим.1 к ст. 272 УК РФ). Эти следы являются материальными невидимыми следами» [3. С. 97].

Поиск цифровых следов, так же, как и следов материального взаимодействия, строится на основе процесса моделирования. В качестве примера можно привести модель рабочего дня среднестатистического горожанина.

Если мысленно прожить свой обычный день, выделяя моменты, когда наши действия инициируют появление цифровых следов, то получится весьма внушительный объем. Даже если у вас не установлена система «Умный дом» или ее элементы (та же интерактивная колонка), информационные технологии всегда сопровождают вас. Например, смартфон (телефонная книга, журналы вызовов, протоколы соединений, логи систем геопозиционирования).

Итак, проснувшись по будильнику (положение с «включено» изменилось на «выключено», включили телевизор (как минимум – изменятся настройки громкости, номер канала, а если это смарт-ТВ, то останется много больше следов), даже микроволновая печь и кофеварка могут иметь цифровое управление и в их памяти также останется след о вас).

За пределами квартиры вы с большой вероятностью попадете в объектив камер отдельных систем видеонаблюдения (от камеры в лифте и на подъезде до видеорегистраторов в автомобилях) или комплексных систем, таких как «Безопасный город».

Оплатив проезд в общественном транспорте или платную парковку банковской картой или приложением на смартфоне, вы также вы также вносите изменения в информационные системы. Пройдя через турникет по пути на работу или учебу, вы снова оставляете след.

С использованием служебной офисной техники ситуация аналогична (компьютеры, карты памяти, сети).

Путь с работы, посещение торговых центров, иных организаций – это все будет сопровождено появлением новых цифровых следов.

Досуг сегодня также связан с использованием цифровых технологий. Посмотрев фильм, просмотрев новости или поиграв в компьютерные игры, вы снова оставляете следы. Умный браслет даже за качеством вашего сна следит!

Как уже говорилось выше, криминалистическое значение имеет вся совокупность следов. В то же время, важно помнить о принципе достаточности. При расследовании преступления необходимо на основе модели произошедшего определять каждый раз, какой объем носителей информации и устройств необходимо исследовать, чтобы собрать достаточное количество информационных следов для установления важных по делу обстоятельств.

В этом процессе важно избежать двух крайностей: с одной стороны – не утонуть в море второстепенной или вовсе ненужной информации, с другой – не упустить важные детали.

Далее кратко проанализируем способы поиска цифровых следов, применяемых сегодня в следственной практике и способах их объективации, легитимации и использования в доказывании по уголовным делам, в том числе, при рассмотрении уголовного дела судом с участием присяжных заседателей.

Учитывая огромное количество возможных цифровых следов необходимо их, прежде всего, классифицировать. В качестве одного из критериев классификации может быть использовано определение того, связан ли этот след непосредственно с объектом преступного посягательства (защищаемая информация) или с орудием совершения преступления (подготовленное специальным образом устройство, которое обеспечило злоумышленнику доступ в защищаемую систему), или такие следы возникли в связи с совершенным преступлением, но ни к орудию преступления, ни к объекту преступного посягательства отношения не имеющие (журнал WI-FI-роутера, который зарегистрировал сотовый телефон преступника в непосредственной близости к месту преступления).

К первой категории мы можем отнести статистическую информацию о деятельности предприятия, направленную ранее в подразделения Инспекции по налогам и сборам. Сюда же относятся данные с камер видеонаблюдения, в зону обзора которых попало место происшествия и пути подхода/отхода преступника.

Во вторую категорию входит вся информация, созданная в результате активных действий лица, совершившего преступление, в ходе подготовки к его совершению (получение несанкционированного доступа в систему), непосредственно во время

совершения преступления (изменение, копирование и удаление данных), а также сразу после совершения, с целью сокрыть следы преступления (очистка системных журналов, удаление следов присутствия в системе и другое).

В третью группу входят следы, связанные с объектом посягательства (фальсифицированные данные бухгалтерского и иных учетов, измененные персональные данные, взломанные защитные программные средства и другие).

В любом случае, поиск цифровых следов начинается с построения следователем (желательно с участием специалиста в области компьютерной информации) мысленной модели произошедшего, которая должна включать все три стадии преступного поведения (подготовка, совершение, сокрытие следов).

С учетом построенной модели проводятся следственные действия, начиная с неотложных, направленных на исключение возможности утраты имеющихся следов. При производстве всех следственных действий, связанных с изъятием носителей информации должен присутствовать специалист в области компьютерной техники.

Фиксация обнаруженных цифровых следов должна производиться в максимально короткий срок, так как данные могут быть изменены, модифицированы. В протоколах следственных действий обязательно указывается время копирования информации, а также системное время устройства, с которого производится изъятие.

В протоколе следственного действия кроме того указываются следующие сведения: устройство, в котором обнаружены виртуальные следы; собственник устройства (если установлен); владелец информации (может отличаться от собственника, если такой установлен), наличие у устройства возможности подключения к сети Интернет или иным телекоммуникационным и локальным сетям и следы такого подключения.

Отдельно должна быть описана операционная система, под управлением которого находится устройство (семейства Windows, Linux, MAC-OC, Android). Должны быть указаны признаки неправомерности использования программного обеспечения, к которым могут относиться наличие программных средств обхода активации, отсутствие фирменных наклеек на корпусе устройства, использование операционной системы MAC-OC на устройствах, произведенных не Apple.

Изъятие обнаруженного цифрового следа и одновременно его фиксация проводятся при обязательном участии специалиста в области компьютерной техники. Наиболее предпочтительным является изготовление специалистом полного образа (виртуальной копии, изготавливаемой с помощью специального программного обеспечения или даже специальных аппаратных средств) осматриваемого носителя информации и производство манипуляций в дальнейшем уде с полученным образом.

После того как цифровой след обнаружен, его, как и другие следы преступления, необходимо подробно описать в протоколе соответствующего следственного действия и изъять. Описание цифрового следа подразумевает знание основ функционирования операционной системы и программного обеспечения, при использовании которого обнаруженный цифровой след возник. Данные сведения может сообщить следователю специалист, участвующий в следственном действии или привлекаемый к участию в уголовном деле.

Изъятие предварительно зафиксированных цифровых следов производится двумя способами: с изъятием устройства – носителя информации (например, компьютера) и с копированием цифровых следов на иные носители.

Важным вопросом является установление владельца изымаемой информации и владельца носителя информации, на котором она была обнаружена. На практике часты ситуации, когда информация хранится пользователями на арендуемом оборудовании, для архивирования данных используются внешние data-центры и так далее. Кроме того, на устройстве подозреваемого может быть обнаружена похищенная или незаконно распространяемая информация, автором и владельцем которой он не является. В целях решения ряда вопросов необходимо связать информацию, носитель информации и владельца информации и носителя данной информации.

Существует несколько способов, которыми можно решить обозначенную задачу:

– владелец устройства и информации участвует в следственном действии и явно указывает (в протоколе следственного действия или отдельном заявлении), что изъятое принадлежит ему, и он готов предоставить подтверждающие это документы;

– в ходе следственного действия или других следственных действий обнаружены документы, в которых прямо поименован конкретный владелец устройства и информации;

– в самих изымаемых данных, а также на устройстве, с которого или с которым они изымаются, имеются сведения, указывающие прямым или косвенным образом на владельца (хранящиеся или ранее удаленные файлы изображений и видеозаписей владельца, идентификатор носителя, на который сохранена информация обнаружен в памяти устройства, принадлежащего конкретному человеку и так далее);

– экспертным путем (автороведческая, трасологическая, генетическая экспертизы и заключения специалистов).

Современные реалии уголовного судопроизводства диктуют необходимость придавать процессу обнаружения, исследования и изъятия доказательств и им самим максимально наглядную форму. В уголовном деле должны содержаться сведения в форме, доступной для восприятия лицами, не обладающими техническим образованием и в форме, доступной для восприятия обывателями с минимальным запасом знаний (присяжные заседатели). Таким образом, мы подошли к следующему разделу лекции – легитимация и объективация доказательств. С данными понятиями вы уже встречались в курсе уголовно-процессуального права (уголовного процесса), однако есть необходимость кратко остановиться на них применительно к процессу использования цифровых следов в раскрытии и расследовании преступлений.

Представление доказательств в суде с участием присяжных имеет определенные отличия от процедуры рассмотрения дела профессиональным судьей. Помимо общих требований, предъявляемых законом к доказательствам: относимости, допустимости и достоверности, – доказательства должны представляться присяжным в максимально понятной для них форме и в объеме, достаточном для формирования необходимого представления о деле и вынесения вердикта. Государственный обвинитель путем представления доказательств должен убедить коллегию в правильности своих выводов, склонить присяжных на свою сторону, сделать их своими единомышленниками.

Для успешного выполнения этой работы, учитывая специфику состава суда и психологические особенности восприятия присяжными заседателями обстоятельств исследуемого события, прокурор должен уметь владеть психологическими

приемами убедительной речи, позволяющими установить с присяжными тесный контакт, вызвать интерес и доверие к себе и своему выступлению.

Для присяжных заседателей представляемые прокурором доказательства должны быть очевидными для восприятия, понятными по содержанию и «прозрачными» по источнику их происхождения.

Указанные рекомендации можно воплотить в жизнь, применяя технические средства в суде (визуальный ряд, слайды, схемы, заслушивание показаний свидетелей, потерпевших, обвиняемых с применением аудио-, видеозаписи и другое).

Опыт поддержания обвинения по такой категории дел показывает, что у присяжных заседателей куда больший интерес вызывает использование в суде, при осуществлении процесса доказывания, элементов наглядности. И, наоборот, при малейшем сомнении в качестве проведенного предварительного расследования или в случае непонимания изложенных им обстоятельств, присяжные выносят оправдательный вердикт. Как правило, сложности доказывания возникают по многоэпизодным и групповым уголовным делам, а также делам экономической направленности, когда от присяжных требуется наличие не только жизненного опыта и здравого смысла при принятии решений, но и специальных познаний в различных сферах человеческой деятельности. Нехватка и сложность понимания поступающей к присяжным от сторон процесса значимой информации вызывают у них внутреннее смятение и неуверенность в правоте обвинения.

Одним из способов объективации доказательств, полученных на основе цифровых следов, является их визуализация. Визуализация данных – это наглядное представление массивов различной информации.

Существует несколько типов визуализации, отличающихся по степени сложности, целевому назначению, функциям. Перечислим основные из них:

– обычное визуальное представление количественной информации в схематической форме. К этой группе можно отнести всем известные круговые и линейные диаграммы, гистограммы и спектрограммы, таблицы и различные точечные графики.

– данные при визуализации могут быть преобразованы в форму, усиливающую восприятие и анализ этой информации. Например, карта и полярный график, временная линия и график с параллельными осями, диаграмма Эйлера;

– концептуальная визуализация позволяет разрабатывать сложные концепции, идеи и планы с помощью концептуальных карт, диаграмм Ганта, графов с минимальным путем и других подобных видов диаграмм;

– стратегическая визуализация переводит в визуальную форму различные данные об аспектах работы организаций. Это всевозможные диаграммы производительности, жизненного цикла и графики структур организаций;

– графически организовать структурную информацию с помощью пирамид, деревьев и карт данных поможет метафорическая визуализация, например, схема Санкт-Петербургского метро;

– комбинированная визуализация подразумевает объединение нескольких сложных графиков в одну схему [2. С. 9].

Подводя итог проведенному исследованию, можно уверенно сказать, что современная криминалистика находится в стадии формирования учения о цифровых следах, нарабатывается понятийный аппарат, устанавливаются междисциплинарные связи.

Исследователи единодушны во мнении о необходимости введения новых терминов, уточнения определений ранее использовавшихся, устранения неоднозначного понимания в рамках разных дисциплин одних и тех же понятий.

Практическая же криминалистика уже сейчас работает с цифровыми носителями информации. Криминалисты трудятся над поиском наилучших способов выявления и фиксации цифровых следов, их исследования, объективации и использования в доказывании.

Список литературы

1. Бастрыкин А. И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий, 2022. URL: //skspba.ru/course/index.php?categoryid=15.

2. Фалилеев В. А. Демонстрационный характер формирования доказательств, представляемых суду присяжных // Законность. 2017. № 8. с. 8–11.

3. Цифровая криминалистика: учебник для вузов / Вехов В. Б. [и др.]; под редакцией В. Б. Вехова, С. В. Зуева. – Москва: Издательство Юрайт, 2022. – 417 с. – (Высшее образование). – ISBN 978–5–534–14600–4. – Текст: электронный //Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/497080.

4. Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / С. В. Зуев [и др.]; ответственный редактор С. В. Зуев. – Москва: Издательство Юрайт, 2022. – 193 с. – (Высшее образование). – ISBN 978–5–534–13286–1. – Текст: электронный // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/497476 (дата обращения: 19.08.2022).

5. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ.

6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

7. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

А. Ю. Чупрова,
доктор юридических наук, профессор,
Всероссийский государственный университет юстиции

ПРОБЛЕМЫ ОТВЕТСТВЕННОСТИ ЗА РАСПРОСТРАНЕНИЕ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ ЛИЧНЫХ ВИДЕОМАТЕРИАЛОВ ИНТИМНОГО ХАРАКТЕРА

Аннотация. Целью работы является исследование проблем уголовной ответственности за оборот личных материалов, содержащих действия сексуального характера, распространенных в виртуальном пространстве помимо воли лица. В статье проводится анализ объективных признаков и предмета рассматриваемой группы деяний, вопросов правовой оценки обращения подобных видеоматериалов в сети Интернет, раскрываются правовые подходы к их квалификации. В результате проведенного исследования были сделаны выводы о целесообразности внесения

изменений в современную судебно-следственную практику, позволяющих устранить имеющиеся противоречия в толковании отдельных законодательных терминов.

Ключевые слова: виртуальное пространство, вымогательство, частная жизнь, порнографические материалы, шантаж, организованная группа, публичная демонстрация

PROBLEMS OF RESPONSIBILITY FOR THE DISTRIBUTION OF INTIMATE PERSONAL VIDEO MATERIALS IN THE VIRTUAL SPACE

Abstract. The purpose of the work is to study the problems of criminal liability for the circulation of personal materials containing sexual acts distributed in the virtual space against the will of the person. The article analyzes the objective features and the subject of the group of acts under consideration, issues of legal assessment of the circulation of such video materials on the Internet, reveals legal approaches to their qualification. As a result of the conducted research, conclusions were drawn about the expediency of making changes to modern judicial and investigative practice, allowing to eliminate the existing contradictions in the interpretation of certain legislative terms.

Keywords: Virtual space, Extortion, private life, Pornographic materials, Blackmail, Organized group, Public demonstration

В последние годы значительный сегмент частной и общественной жизни человека переместился в виртуальное пространство. Особенно заметным это стало в период пандемии, когда на карантин отправлялись граждане целых государств со строгой установкой своих правительств не покидать место проживания без специального разрешения или, в виде исключения, в связи со значимостью для социума и экономики страны определенных видов деятельности. Но человек – существо социальное и ему необходимо общение, он хочет знакомиться, устанавливать дружеские или романтические отношения, просто приятно проводить время. И в это тяжелое время ему на помощь пришел Интернет, оказавший поддержку во многих вопросах, в том числе сугубо личного характера.

Всероссийский центр изучения общественного мнения в 2018 г. провел опрос на тему, какие способы устройства личной жизни наиболее востребованы в нашей стране. С помощью Интернета на сайтах знакомств в социальных сетях пытались устроить личную жизнь 22 % респондентов в 2015 г. и 19 % респондентов – в 2019 г. При этом 58 % опрошенных, имевших личный опыт обращения на разные сайты знакомств, считали этот способ поиска счастья эффективным [1].

Среди зарубежных пользователей отношение к сайтам знакомств аналогично высказанным российскими респондентами. Согласно проведенным в 2020 г. Pew Research Centre исследованиям трое из десяти взрослых американцев пользовались приложениями или сайтами для знакомств, хотя этот показатель во многом зависит от возраста и сексуальной ориентации. Среди молодых людей в возрасте до тридцати лет каждый второй (48 %) пользовались сайтами для знакомств, среди лиц в возрасте до 49 лет – 38 %, для тех, кому за пятьдесят только 16 % посещали подобные сайты. Представители сексуальных меньшинств в два раза чаще, нежели остальные американцы использовали платформы знакомств (55 % против 28 %) [2].

Лабораторией Касперского в результате опроса нескольких тысяч Интернет-пользователей из 30 стран получены аналогичные данные: каждый третий взрослый является посетителем сайтов знакомств.

Цели посещения подобных платформ назывались разными, но 13 % посетителей интересуют исключительно сексуальные аспекты. 18 % мужчин и 5 % женщин использовали такие сайты в целях поиска сексуальных партнеров [3].

Проведенное американским центром исследование также показало, что Интернет расширил границы общения, в том числе и с эротическими подтекстами. Для сексуальных игр непосредственно в сети Интернет использовались различные варианты связи. Однако настоящую революцию произвели веб-камеры, позволяющие создать эффект присутствия участников сексуальных действий. Секс в интернет-пространстве стал доступным для многих, и значительное число людей, особенно в период пандемии, стали постоянными участниками таких встреч. Вместе с тем сексуальные развлечения в онлайн формате доставляют не только удовольствия, но и несут определенные угрозы. Рассмотрим несколько различных ситуаций, повлекших серьезные проблем, многие из которых не доходят до правоприменителей полностью или частично, создавая новые сегменты латентной киберпреступности.

Недавний скандал с известным российским футболистом стал достоянием общественности в силу того, что в Интернет были выложены его интимные видеоматериалы, на которых он выступает стороной онлайн-сексуальных отношений. В то же время, материалы, запечатлевшие его партнершу, во всемирной паутине отсутствуют. Очевидно, что знаменитость попала в силки, расставленные охотниками за состоятельными представителями обоего пола, не отказывающимися от сексуальных развлечений в онлайн-формате в режиме реального времени. Такие встречи сопряжены с серьезными рисками, одним из которых является угроза распространения материалов интимного характера в Интернет. Последствия обнародования подобной информации могут быть самыми разнообразными, от репутационных проблем до вынужденного оставления места работы. В ситуации с известным футболистом видеоматериалы личного характера стали катализатором не самых лучших перемен в его жизни.

Информация об аналогичных, хотя и не настолько громких онлайн-встречах интимного характера периодически появляется в информационных источниках, однако реакция правоприменителей далеко не всегда становится достоянием общественности. Чаще всего действия участников и распространителей видеоконтента остаются безнаказанными. Однако их поведение содержит признаки нескольких самостоятельных преступлений, поскольку посягает на несколько самостоятельных объектов, охраняемых уголовным законом.

В тех случаях, когда изготовители видеоматериалов интимного характера в качестве условия их сокрытия от пользователей сети Интернет выдвигают требования имущественного характера, их поведение посягает на собственность потерпевшего и содержит признаки шантажа, одного из видов такого серьезного преступления как вымогательство. Под шантажом понимают выдвижение требований передачи денежных средств, имущества, совершения действий имущественного характера под угрозой разглашения сведений, порочащих потерпевшего или иных сведений,

распространение которых может причинить существенный вред правам или законным интересам потерпевшего либо его близких. Можно ли в подобной ситуации признать видеоматериалы интимного характера в качестве порочащей потерпевшего информации или отнести их к иной информации, распространение которой может причинить существенный вред правам или законным интересам потерпевшего. Действительно, с учетом сложившихся в обществе представлений о культуре интимных отношений, новые веяния сексуального характера воспринимаются в обществе весьма неоднозначно и могут негативно сказаться на отношениях в семье, с друзьями и родственниками, создать сложности в рабочем коллективе, в отношениях с руководством, закрыть перспективы карьерного роста. Во всяком случае, проведенное автором интервью 39 респондентов с высоким уровнем образования, разных возрастных групп и профессий, позволило определить основные тренды в восприятии подобного рода угроз, хотя и в гипотетическом ракурсе. Следует отметить, что все опрошенные отвергли саму возможность участия в подобных видео сессиях. Тем не менее, согласились ответить на несколько вопросов. Респонденты (39 человек), независимо от возраста и пола, восприняли информацию подобного рода как информацию, хотя и не позорящую, но, безусловно, причиняющую существенный вред законным интересам любого человека. 87 % (34 человека) отметили, что такой опыт негативно скажется на отношениях в семье, 95 % (37 человек) увидели сложности в последующих отношениях в рабочем коллективе. В действиях лиц, требующих передачи денежных средств под угрозой распространения материалов интимного характера, полученных в результате видеосъемок сеанса киберсексуальных отношений, все респонденты усмотрели признаки вымогательства, осуществляемого путем шантажа, т. е. требования передать определенную сумму денежных средств под угрозой распространения информации, способной причинить существенный вред законным интересам человека. Однако 62 % (24 человека) выразили готовность скорее заплатить шантажистам (если позволят материальные возможности), нежели претерпеть все отрицательные последствия такого опыта.

Вместе с тем не все пострадавшие от действий шантажистов переводят им требуемые денежные средства. Но для квалификации вымогательства, как оконченного преступления, не имеет значения, получил ли вымогатель запрошенную сумму. Поскольку вымогательство считается оконченным преступлением с момента предъявления требования о передаче определенной суммы денег, сам факт получения их вымогателем не влияет на правовую оценку содеянного [4].

Следует отметить, что по материалам средств массовой иформации чаще всего подобные преступления выполняются группами, имеющими стабильный состав, в течение длительного времени, четко распределив между собой роли [5]. Действия субъектов выполняются в данном случае организованной группой. Исходя из п. 15 постановления Пленума Верховного Суда Российской Федерации от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое», организованной группе присущи, в частности, такие признаки как устойчивость, наличие в ее составе организатора и заранее разработанного плана совместной преступной деятельности, распределение ролей между участниками группы при подготовке к совершению преступления и осуществлении преступного умысла. Особое внимание

следует обратить на то, что современная судебная практика рассматривает любого участника группы, совершающей вымогательства с использованием материалов, полученных в результате сеансов киберсекса, как исполнителя рассматриваемого преступления [6].

Таким образом, эти действия можно квалифицировать как вымогательство, выполненное под угрозой распространения информации, причиняющей вред законным интересам лица, совершенное организованной группой, которая специализируется на шантаже в виртуальном пространстве (п. «а» ч. 3 ст. 163 УК РФ). Как видим, речь идет о совершении особо тяжкого преступления, и поэтому не совсем понятен столь незначительный интерес правоприменительных органов к подобным деяниям вымогателей.

Помимо отношений собственности, действия участников таких групп посягают на общественную нравственность, поскольку затрагивают нравственные представления в сфере сексуальных отношений, которые отражают укоренившиеся в сознании людей взгляды о границах дозволенного при изображении или описании обнаженного тела человека и его сексуального поведения [7. С. 114]. Поэтому в поведении распространителей интимных видеоматериалов прослеживается не только вымогательство, но и распространение порнографических материалов. Хотя в уголовно-правовой доктрине отмечается, что порнографию нельзя определить только по формальным признакам, необходимо применять в совокупности оценочные категории и формальные критерии [8. С. 18], тем не менее в подобных материалах крупным планом демонстрируются гениталии человека, совершающего действия сексуального характера, что позволяет отнести эти материалы к числу порнографических. Рассылка порнографических материалов осуществляется в информационно-телекоммуникационной сети Интернет, получение личных интимных видеоматериалов представляет собой результат совестных усилий членов группы, поэтому действия всех участников такого криминального проекта можно квалифицировать по п. «а», «б» ч. 3 ст. 242 УК РФ, как распространение порнографических материалов, совершенное организованной группой с использованием сети Интернет.

В ч. 1 ст. 23 Конституции Российской Федерации указано, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Действия же распространителей личного интимного контента грубо нарушают конституционное право каждого человека на неприкосновенность его частной жизни. Исходя из предписаний Конституции РФ, конфиденциальным характером обладает любая информация о частной жизни лица, поэтому она во всех случаях относится к сведениям ограниченного доступа. Как отмечается Конституционным Судом Российской Федерации, право на неприкосновенность частной жизни, личную тайну «означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера» [9], С позиции Конституционного Суда РФ в понятие частная жизнь включается та область жизни человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если носит непротивоправный ха-

рактер [10]. Все вопросы интимной жизни человека, его сексуальных предпочтений (если они не нарушают закон) следует рассматривать как его частную жизнь, сведения о которой могут раскрываться только им самим. В противном случае его конституционное право будет грубо и неизвинительно нарушено. Исходя из этого, можно сделать вывод, что действия лиц, разместивших в сети Интернет интимный контент без согласия лица, содержат признаки ч. 1 ст. 137 УК РФ, предусматривающей ответственность за незаконное распространение сведений о частной жизни лица, составляющих его личную тайну без его согласия.

Помимо рассмотренной выше ситуации, связанной с онлайн-сексом, можно встретить и иные нарушения прав граждан и российского законодательства. Рассмотрим еще один пример. Женщина познакомилась с молодым человеком при помощи международной службы знакомств. Постоянное общение между ними в онлайн-формате в режиме реального времени перешло в сексуальные отношения с использованием вэбкамеры. Через какое-то время партнер сообщил женщине, что их интимные встречи в режиме реального времени демонстрировались другим людям. В этом случае, вряд ли можно утверждать, что в поведении партнера отсутствует состав преступления, как утверждали правоприменители, к которым женщина обратилась за помощью. Исходя из формальных признаков видеоматериалы, которые предназначались для мужчины, имели глубоко личный и интимный характер. Сложившиеся между мужчиной и женщиной отношения не были рассчитаны на участие третьих лиц, поэтому женщина вела себя достаточно раскованно. В этом случае, также как и в рассмотренном ранее, присутствует нарушение неприкосновенности частной жизни, а также, по формальным основаниям, содержатся признаки публичной демонстрации порнографических видеоматериалов в режиме реального времени, которая характеризуется в данной ситуации открытым показом порнографических материалов в прямом эфире определенной группе лиц, но без предоставления участникам просмотра возможности самостоятельно использовать эти материалы (именно возможность самостоятельного использования порнографических материалов потребителями отличает распространение от их публичной демонстрации).

Таким образом, резюмируя вышеизложенное, можно сделать вывод о том, что нарушение приватности сексуальных контактов в киберпространстве посягает не только на неприкосновенность частной жизни, но и общественную нравственность, поэтому содеянное может квалифицироваться по совокупности ч. 1 ст. 137 и п. «б» ч. 3 ст. 242 УК РФ, как нарушение неприкосновенности частной жизни и публичная демонстрация порнографических материалов в сети “Интернет”.

В тех случаях, когда имеет место вымогательство и интимные видеоматериалы выкладывается в сеть, поведение виновных содержит, помимо вымогательства, нарушение неприкосновенности частной жизни и распространение порнографических материалов в сети интернет.

Список литературы

1. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/lyubov-nechayanno-nagryanet (дата обращения: 7.09.2022)

2. Vogels E. A. 10 facts about Americans and online dating. URL: https://www.pewresearch.org/fact-tank/2020/02/06/ (дата обращения: 17.08.2022).

3. Dangerous Liaisons: is everyone doing it online? URL: https://www.kaspersky.com/blog/online-dating-report/ (дата обращения: 17.08.2022).

4. Постановление Пленума Верховного Суда РФ от 17.12.2015 № 56 «О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации)» (информационная система «Гарант»).

5. Секс по Интернету вытесняет привычные отношения между полами // Московский комсомолец. 19.09.2014; Деньги или позор: как россияне попадают в сети секс-шантажистов/НТВ.03.03.2022 г. URL: https://www.ntv.ru/novosti/2688051/

6. Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 29.06.2021) «О судебной практике по делам о краже, грабеже и разбое» (информационная система «Гарант»).

7. Булгакова О. А. Уголовная ответственность за распространение порнографических материалов или предметов: дис. … канд. юрид. наук. Ставрополь, 2003. 178 с.

8. Джинджолия Р. С. Уголовная ответственность за незаконное распространение порнографических материалов или предметов. Москва; Сочи, 2001. 65 с.

9. Определения Конституционного Суда Российской Федерации от 9 июня 2005 г. № 248-О «Об отказе в принятии к рассмотрению жалобы гражданина Захаркина В. А. и Захаркиной И. Н. на нарушение их конституционных прав п. «б» ч. 3 ст. 125 и ч. 3 ст. 127 Уголовно-исполнительного кодекса Российской Федерации».

10. Определение конституционного Суда Российской Федерации от 28 июня 2012 г. № 1253-О «Об отказе к рассмотрению жалобы гражданина Супруна М. Н. на нарушение его конституционных прав ст. 137 УК РФ».

Р. К. Шаймуллин,
кандидат юридических наук, доцент
Оренбургский государственный университет

ОТДЕЛЬНЫЕ АСПЕКТЫ ЦИФРОВИЗАЦИИ ПРАВОВЫХ ОСНОВ БОРЬБЫ С КОРРУПЦИЕЙ

Аннотация. В статье дан краткий анализ состояния и перспектив отдельных направлений цифровизации правовых основ борьбы с коррупцией. Показаны исторические и современные проблемы, связанные с цифровизацией основ борьбы с коррупцией, не только ее конституционно-правовой основы, но и возможных злоупотреблений с использованием цифровых технологий как коррупциогенное условие в социуме. Особое внимание в статье уделяется новому Национальному плану противодействия коррупции на 2021–2024 годы, содержащему отдельный раздел о цифровизации борьбы с коррупцией.

Ключевые слова: право, цифровизация права, коррупция, борьба с коррупцией, антикоррупционное законодательство, конституционные основы борьбы с коррупцией, коррупциогенное условие

SEPARATE ASPECTS OF DIGITALIZATION OF THE LEGAL FRAMEWORK FOR ANTI-CORRUPTION

Abstract. The article provides a brief analysis of the state and prospects of certain areas of digitalization of the legal framework for the fight against corruption. The historical and modern problems associated with the digitalization of the foundations of the fight against corruption, not only its constitutional and legal basis, but also possible abuses using digital technologies as a corruption-generating condition in society, are shown. Particular attention is paid to the new National Anti-Corruption Plan for 2021–2024, which contains a separate section on the digitalization of the fight against corruption.

Keywords: Law, Digitalization of law, Corruption, Fight against corruption, Anti-corruption legislation, Constitutional foundations for the fight against corruption, Corruption-causing condition

Цифровизация общественных отношений неизбежно затрагивает, в том числе, и антикоррупционную политику социума. С одной стороны, это касается всех сторон и аспектов, касающихся «классических» подходов борьбы с этим негативным явлением, начиная от выработки концепций борьбы до вопросов реализации санкций за коррупционные правонарушения. С другой стороны, само явление цифровизации антикоррупционной политики неизбежно будет ставить вопросы «нового» уровня, учитывающего эти особенности, так сказать как «вещь в себе». Новый Национальный план противодействия коррупции на 2021–2024 гг., утвержденный Президентом Российской Федерации 16.08.2021, содержит отдельный Раздел XVI «Применение цифровых технологий в целях противодействия коррупции и разработка мер по противодействию новым формам проявления коррупции, связанным с использованием цифровых технологий», в котором определены отдельные направления борьбы с коррупцией в российском обществе с использованием цифровых технологий как в традиционных сферах уже существующих в антикоррупционном законодательстве, так и определяются новые подходы и тренды для правоприменителя [3].

Достижения современных технологий, однозначно стали одним из решающих факторов в решении вопросов борьбы с пандемией COVID-19, когда цифровые технологии стали использоваться среди широких слоев населения с целью упорядочения движения. Попытки внедрения так называемого QR-кода для посетителей торговых центров, пассажиров общественного транспорта в ряде городов (Москва, Казань и др.), блокировка электронных проездных билетов для лиц пенсионного возраста и т.д., показало определенные очертания будущего формата отношений lex de futuro. Анализируя опыт проходивших попыток использования цифровых технологий в условиях прошедшей пандемии, можно сделать вывод, что он вобрал в себя все фундаментальные диалектические законы основ существования и развития общественных отношений, показав тем самым, что «цифровизация» как и «информатизация», «интернетизация» и т.д. является лишь ступенью в ряду обработки и передачи информации, как описывали в своих трудах специалисты – кибернетики [1. С. 99–100].

Как указывает Нестеров А. В.: «Цифровизация не может осуществляться без законодательного регулирования, а оно само уже не может обходиться без цифровизации, в том числе без цифрового законодательства. Любая автоматизация подразумевает не только формализацию, унификацию, стандартизацию, но и устранение бюрократических барьеров» [2. С. 45].

В рамках вышеуказанных «унификации и стандартизации», следует указать на проблемы, которые стоят перед российским обществом как частью мирового сообщества в решениях задач по борьбе с коррупцией. В связи с развитием антикоррупционной политики в России на протяжении последних 30–40 лет, борьба с коррупцией вступила в острую фазу и объективно стала соответствовать международным стандартам. Невозможность обойтись внутринациональными социально-правовыми инструментами в области борьбы с коррупцией, ратификация (за исключением некоторых положений Конвенции ООН 2003 г. против коррупции), привела к тому, что Россия взяла курс на выстраивание цивилизованной перспективной политики развития российского общества без коррупции.

Рассмотрим более глобальный тренд борьбы с коррупцией, который приводит С. Н. Шевердяев в своей монографии, выделяя три глобальных временных отрезка: первый – с середины XIX в. по 1970-е гг., с середины 1970-х гг. по конец XX в., и с начала XXI в. по нынешнее время [5. С. 14]. Следует отметить, что вышеуказанные временные исторические этапы борьбы с коррупцией также сопровождались бурным развитием информационных технологий, призванных и должных осуществлять «прозрачность» общественных и управленческих отношений, однако, вместе с этим, повысивших массовое манипулирование общественным сознанием и приведших к «оболваниванию» масс, войнам и катастрофам, поскольку «системные» ошибки теоретиков, лежащие в основе этих новых законов приводили к искаженному пути построения и новых правопорядков, как говорится, «благими намерениями дороги были выстроены в ад». Ускорение процессов информатизации приводило не только к распространению гуманитарных процессов просветительского порядка, наоборот, к повышению уровня злоупотреблений средствами массовой информации и, как следствие, манипулированию массовым сознанием. Кибернетизация общественных отношений вместе с повышением уровня их информатизации повышает также уровень коррупционных отношений с помощью цифровизации. Например, проведение электронных торгов в рамках программ государственных закупок вовсе не решает проблемы «изощренности» в подмене и качестве поставок товаров и услуг, злоупотреблений при проведении данных торгов, а, наоборот, повышает уровень и плотность таких отношений как «непотизм», «местничество» и «очковтирательство», явлений, которые клеймились позором во все времена (и в том числе, в недалеком прошлом – в Советский период развития отечественной истории). Как справедливо задает вопрос С. А. Авакьян в коллективной монографии, посвященной вопросам коррупции: «Почему при почти идеальных конституционных основах общественного и государственного развития, при неуклонном принятии и реализации мер борьбы с коррупцией она существует и продолжает разъедать, разрушать и систему как таковую, и сознание граждан, все более наполняющихся неверием в способность этой самой конституционно-политической системы обеспечить не только успешное движение впе-

ред по пути прогресса, но и спасти самое себя от ржавчины, покрывающей формальные конституционные ценности?», предлагая, затем, анализировать корень коррупционных проблем в самих главных составляющих общественного бытия в стране: 1) публичную власть; 2) собственность; 3) государство [4. С. 18].

Как можно заметить, эти основные элементы конституционного строя присутствуют и будут присутствовать в социуме независимо от уровня их цифровизации, поскольку представляют ценность при существовании самого человеческого бытия, доказывая их фундаментальность для таких положительных явлений как сама цифровизация, так и негативных явлений, таких как корруцпия, доказывая их производный характер по отношению к вышеуказанному базису общества, облеченных в конституционно-правовую оболочку. Развитие институтов антикоррупционной политики – внедрение антикоррупционных стандартов в рамках службы, антикоррупционной экспертизы нормативно-правовых актов и их проектов, антикоррупционное декларирование доходов и расходов служащих и других мер антикоррупционного характера, независимо от уровня их цифровизации, носит объективный характер, которое также исторически формировалось на протяжении столетий, доказывая их социальное предназначение в борьбе с коррупцией в сущностном содержании.

Поэтому, в свою очередь, на основе анализа борьбы с коррупцией, хотелось бы заметить, что основные законы диалектики всегда, независимо от уровня развития информационных процессов и цифровизации, предполагают существование постоянной борьбы явлений и процессов как противоположностей, в том числе внутри социума. В любом случае, коррупция присутствует и в реальности и в цифровой оболочке. Все формы классических правонарушений (преступлений), содержащих коррупционные признаки будут существовать и при их оцифровке. Это будет ставить новые задачи перед специалистами не только в области борьбы с коррупцией, но и в области юриспруденции для формулирования правильных и грамотных, юридически обоснованных, содержащих изначально антикоррупционные рецепты путей решения социальных проблем.

Список литературы

1. Абдеев Р. Ф. Философия информационной цивилизации. М.: Владос, 1994. С. 99–100.

2. Нестеров А. В. Цифровая трансформация юридической деятельности и законодательства // Правовое государство: теория и практика. 2020. № 4 (62). Часть 1. С.45.

3. О Национальном плане противодействия коррупции на 2021–2024 годы: Указ Президента РФ от 16.08.2021 № 478. URL: http://www. http://www.consultant.ru/document/cons_doc_LAW_392999/be374c4d18d96b8a38c10685d1056efa5924bd56/ (дата обращения: 18.09.2022).

4. Противодействие коррупции: конституционно-правовые подходы: коллективная монография / отв. редактор и руководитель авторского коллектива доктор юридических наук, профессор С. А. Авакьян. М.: Юстицинформ, 2016. С. 18.

5. Шевердяев С. Н. Отражение современной антикоррупционной культуры в российском конституционном праве. М.: Юстиц-Информ, 2020. С. 14.

К. В. Шевелева,
старший преподаватель,
МИРЭА – Российский технологический университет

О РАСПРОСТРАНЕНИИ СЛУЧАЕВ РЕАБИЛИТАЦИИ НАЦИЗМА В СОЦИАЛЬНЫХ СЕТЯХ ЦИФРОВОЙ СРЕДЫ

Аннотация. За последние несколько лет преступность в цифровом пространстве существенно трансформировалась, поскольку Интернет, в том числе, социальные сети, стали играть существенную роль в жизни общества. Все большую актуальность приобретают посягательства на историю Великой Отечественной войны, а также пропаганда и оправдание нацистской идеологии, совершенных посредством социальных сетей. Рост совершения указанных противоправных действий в социальных сетях свидетельствует о неэффективности современного правового регулирования данной сферы, обуславливает актуальность проведения исследований по этой тематике. Автором рассмотрены социальные сети, как источник преступной ложной информации о событиях ВОВ, проанализировано влияние такой информации на молодое поколение, а также изучены способы ее распространения в цифровом пространстве. В результаты предложены меры противодействия реабилитации нацизма и фальсификации отечественной истории, совершенных с использованием социальных сетей.

Ключевые слова: реабилитация нацизма, фальсификация истории ВОВ, цифровые технологии, социальные сети, сеть Интернет, историческая память, оправдание и пропаганда нацизма

ON THE SPREAD OF CASES OF THE REHABILITATION OF NAZISM IN THE SOCIAL NETWORKS OF THE DIGITAL ENVIRONMENT

Abstract. Over the past few years, crime has largely transformed, as the Internet, including social networks, began to play a significant role in society. Encroachments on the history of the Great Patriotic War, as well as propaganda and justification of the Nazi ideology, committed through social networks, are becoming increasingly relevant. The growth in the commission of these illegal actions in social networks indicates the inefficiency of modern legal regulation of this area, and determines the relevance of conducting research on this topic. The author considers social networks as a source of criminal false information about the events of the Second World War, analyzes the impact of such information on the younger generation, and also studies the ways of its dissemination in the digital space. As a result, measures are proposed to counteract the rehabilitation of nazism and the falsification of national history, committed using social networks.

Keywords: Rehabilitation of nazism, Falsification of the history of the Second World War, Digital technologies, Social networks, the Internet, Historical memory, Justification and propaganda of nazism

Стремительное развитие цифровой среды предопределяет все большую интеграцию материального мира граждан в виртуальное пространство. Мессенджеры,

социальные сети, интернет-сайты становятся неотъемлемой частью жизнедеятельности любого современного человека, выполняя коммуникативную, развлекательную, познавательную и другие функции. Однако помимо позитивного влияния цифровой среды, нельзя не отметить и ее негативное воздействие на общество с точки зрения распространения преступной деятельности в интернет – пространстве, и влияния такой деятельности на внутриполитическую обстановку Российской Федерации.

Значимое место в цифровой среде для граждан имеют социальные сети. Прежде всего, необходимо отметить, что за последние двадцать лет социальные сети приобрели не только социальное, но и политическое значение, поскольку в настоящий момент они выполняют скорее функцию средств массовой информации, а чаще – дезинформации. И такое положение постепенно превратило их в своего рода «оружие», которое активно используется против государственной политики, направленной, в том числе и на противодействие реабилитации нацизма, а также на сохранение исторической памяти народов Российской Федерации о событиях Великой Отечественной войны. Между тем, в Стратегии национальной безопасности РФ указано, что в целях единения и укрепления народов Российской Федерации в стране установлен режим правовой охраны исторической памяти, что способствует сохранению исконных общечеловеческих основ и социально важных ориентиров общественного формирования. Стремление исказить отечественную историю приравнивается к способам размывания традиционных российских духовно-нравственных ценностей и ослабления единства многонационального народа Российской Федерации, что представляет собой одну из угроз национальной безопасности [8].

Отметим, что среди духовно-нравственных ценностей россиян особое место занимает историческая память о Великой Отечественной войне. Вместе с тем вот уже более 75 лет не прекращаются попытки фальсификации ее истории, что неуклонно способствует распространению случаев оправдания и пропаганды нацизма. Согласимся с С. А. Куликовой, что «установление государственной мемориальной концепции на конституционном уровне призвано решить задачи по определению аксиологических основ развития общества, формированию национального самосознания, сохранению культурной идентичности и духовно-информационного суверенитета. Высокая социальная значимость регулируемых общественных отношений, их относительная обособленность и внутреннее структурное единство дают основание сделать вывод о формировании нового конституционно-правового института охраны исторической памяти» [1. С. 71].

Российская Федерация приняла ряд нормативных правовых актов, направленных на противодействие фальсификации истории и препятствование оправдания и пропаганды нацизма, во главе с поправками в Конституцию РФ в 2020 г., которые обеспечивают защиту исторической правды. Так, в 2021 г. был принят Федеральный закон, который направлен на увековечивание Победы, установивший ряд запретов на дискредитацию деятельности руководства СССР, командования и военнослужащих Советского Союза в период Великой Отечественной войны [9]. Кроме того, в 2014 г. законодатель установил уголовную ответственность за деяния, связанные с реабилитацией нацизма [10]. Согласно статье 354^1 УК РФ ответственность наступает в случае отрицания фактов, установленных приговором Международного

военного трибунала для суда и наказания главных военных преступников европейских стран оси, одобрения преступлений, установленных указанным приговором, а равно распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны, совершенных публично [7].

Особо отметим, что в 2021 г. статью 354[1] УК РФ существенно модернизировали, включив изменения, в соответствии с которыми в правовую норму введены деяния, направленные на защиту ветеранов Великой Отечественной войны от преступных посягательств. Помимо этого, указанную статью дополнили некоторыми новыми квалифицирующими признаками, включая совершение деяния с использованием информационно – телекоммуникационных сетей, в том числе сети Интернет [11].

Необходимость включения использования информационно – телекоммуникационных сетей, в том числе сети Интернет, как квалифицирующего признака, обусловлено тем, что такая противоправная деятельность в большей степени осуществляется в цифровом пространстве. В первую очередь, это связанно с геополитической обстановкой в мире и стремлением руководства некоторых стран (США, Западная Европа, Украина) дискредитировать роль СССР в победе над Гитлером, а трансграничный характер сети Интернет позволяет распространить любую информацию среди широких масс вне зависимости от места отправления такой информации. В тоже время, современные возможности поисковых систем в сети с использованием служб индексирования существенно облегчают пользователям доступ к распространяемой информации, даже если содержание такой информации противоправно.

Подчеркнем, что наибольший контингент пользователей сети Интернет, включая социальные сети, составляют молодые люди возраста до 35–40 лет. И поскольку современная молодежь чаще интересуется различным развлекательным интернет – «контентом», нежели отечественной историей, то они и становятся жертвами информационного негативного потока, идущего от лиц (в том числе и из-за рубежа), посягающих на историческое наследие Российской Федерации и пропагандирующих нацизм, фашизм.

В качестве примера негативного воздействия на молодежь укажем на интервью с российским рэп-исполнителем – Моргенштерном[1], размещенном: 26.10.2021 на видео-хостинге YouTube[RU]. В процессе диалога с ведущей, музыкант Моргенштерн позволил себе высказывание в отношении государственного ритуала празднования Великой Победы, а именно о нецелесообразности финансирования мероприятий, проводимых ежегодно 9 мая, отметив их слишком «помпезный», «консервативный» и «нафталиновый» характер [2]. Публичное высказывание исполнителя вызвало молниеносную реакцию у общественности, которые обратились в Генеральную Прокуратуру Российской Федерации с требованием привлечь Моргенштерна к уголовной ответственности (ч. 3 ст. 354[1] УК РФ «Реабилитация нацизма»).

По нашему мнению, в деяниях музыканта не усматриваются признаки преступления, предусмотренные вышеназванной статьей Уголовного кодекса Российской

[1] 06.05.2022 Министерство Юстиции Российской Федерации признало Моргенштерна (Алишера Валеева) физическим лицом – иностранным агентом, т. е. лицом, которое, осуществляя свою деятельность, получает иностранную поддержку в виде финансирования. (Прим. автора).

Федерацией, что исключает уголовную ответственность. Вместе с тем, учитывая, что интервью музыканта посмотрело 8,2 млн пользователей видео-хостинга, и в ряду поклонников артиста наибольший контингент занимают школьники, можно сделать вывод о том, что заявление Моргенштерна потенциально способно оказать влияние на ценность Дня Победы.

Причем молодежь не всегда выступает жертвой такого рода воздействия. Нередко отсутствие понимания истинного значения Победы советской армии в Великой Отечественной войне, невозможность фильтрации негативной информации в сети Интернет о деятельности СССР в годы Войны, а также неограниченные возможности интернет- пространства порождают совершение юношами и девушками целого ряда аморальных поступков, квалифицируемых уголовным законодательством Российской Федерации как преступления против мира и безопасности человечества. Так, широкое распространение среди интернет- аудитории получила видеозапись, где на фоне могилы Неизвестного Солдата в городе Москве совершался «однополый половой акт». Участниками ролика являлись известные среди молодежи блоггеры, которые, вероятно, вдохновились актуальными на тот момент веяниями пренебрежения к памятникам советской истории и в целях «хайпа» разместили видеозапись в социальных сетях. В отношении них возбуждено уголовное дело по признакам преступления, предусмотренного ч. 3 ст. 354[1] УК РФ (осквернение символов воинской славы) [6].

В качестве еще одного примера представим уголовное дело в отношении 19-летнего М. Юферова, возбужденное по признакам преступления, предусмотренного ч. 4 ст. 354[1] УК РФ. 25.11.2021 осужденный, находясь на объекте мемориального значения, осквернил стенд, посвященный ветерану Великой Отечественной войны гвардии – лейтенанту Фролову Анатолию Александровичу. В момент совершения деяния преступник осуществлял видеозапись, которую впоследствии разместил в социальной сети и распространил среди пользователей. Правоприменитель квалифицировал данное деяние как посягательство на общественные отношения, гарантирующие сохранение и уважение к исторической памяти народов Российской Федерации о событиях ВОВ, причем использование осужденным информационно-телекоммуникационных сетей, в том числе сети Интернет для распространения видеоролика усилило ответственность [5].

Итак, как видится из вышеназванных примеров, Интернет становится не только источником деструктивной информации, но и местом реализации преступного умысла, причем виртуальное пространство социальных сетей играет роль «места совершения преступления».

В тоже время в социальных сетях используются различные способы размещения и распространения информации. Исследователь Ю. С. Пестерева выделяет следующие наиболее распространенные способы обмена информацией: «посты», «скриншоты», «репосты», «лайки». Объединяет указанные способы обязательное наличие содержания, т. е. той или иной информации, вызывающей у автора определенный интерес [3. С. 113].

Изучая судебную практику по делам о реабилитации нацизма, отмечаем, что большинство преступлений совершаются на платформах социальных сетей выше-

названными способами. В рассмотренных нами уголовных делах «скриншоты», «посты», «лайки» и «репосты» расцениваются правоприменителем как личное высказывание, влекущее общественную опасность. В частности, 24.12.2014 В. Лузгин, имея умысел на распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны среди неограниченного круга лиц, разместил в социальной сети репост статьи под названием «15 фактов про «бандеровцев», или о чем молчит кремль», где сообщалось, что войну, совместно с Германией развязало руководство Советского Союза, причем сделан акцент на «тесном сотрудничестве» коммунизма и нацизма [4]. Действия Лузгина квалифицированы по ч. 1 ст. 354[1] УК РФ ввиду того, что его репост был приравнен к выражению личного мнения и направлен на отрицание фактов, установленных приговором Международного военного трибунала.

Как видим, если лицо высказывает публично, в том числе и в социальной сети, одобрение преступлений, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси, отрицает факты, установленные указанным приговором, то он совершает преступление вне зависимости от цели и мотивов совершенного деяния, даже если опубликованная информация является необдуманным «ретвитом»[1] другого человека.

В свою очередь, большинство обвиняемых по исследуемой статье не осознают всю тяжесть совершенных ими деяний, предполагая, что такая информация – это лишь популяризация своего мнения в Интернете, и общественную опасность такая информации не представляет. Подобная позиция, с точки зрения уголовного права ошибочна, однако требует детальной проработки со стороны законодателя. Это связанно с тем, что лица, совершившие преступление посредством социальных сетей в целях реабилитации, оправдания и пропаганды нацистской и фашистской идеологий несут одинаковую ответственность с лицами, совершившими такого рода преступления в Интернете в иных целях (хулиганства, «хайпа», вандализма и т. д.). По-нашему мнению, такие деяния необходимо разграничить ввиду того, что в первом случае объектом преступлений действительно становится мир и безопасность человечества, а во втором – такие преступления посягают скорее на общественную нравственность.

Итак, социальные сети, безусловно, являются неотъемлемой частью жизни современного общества. В настоящий момент они выступают как новая область человеческого взаимодействия, но зачастую это взаимодействие сопряжено с осуществлением противоправной деятельности, в том числе в сфере оправдания, пропаганды и реабилитации нацизма. Популярные социальные сети становятся местами распространения ложной информации об истории Великой Отечественной войны и деятельности руководства СССР в это время. Помимо указанного, неограниченная информация в социальных сетях способна подталкивает пользователей к совершению преступлений против исторической памяти народов Российской Федерации о событиях середины XX в., а в конечном итоге привлекает позитивное внимание молодежи к явлениям нацизма, фашизма. Все это дестабилизирует

[1] Ретвит – вторичная публикация сообщения, размещенного другим пользователем в сети Интернет, со ссылкой на источник (Прим. автора).

внутриполитическую обстановку в стране, деструктивно влияет на население Российской Федерации, размывая историко – культурный код общества, являющийся главной исторической ценностью, объединяющей людей разных национальностей, социальных и возрастных групп.

Исходя из изложенного, в целях противодействия распространению преступлений, предусмотренных ст. 354[1] УК РФ, совершенных с использованием социальных сетей, предлагаем:

Во-первых, детализировать признаки субъективной стороны реабилитации нацизма, включив в диспозицию статьи указание на цель совершенного деяния, а именно: «в целях оправдания и пропаганды идеологий нацизма, фашизма»;

Во-вторых, создать цельную систему противодействия распространению ложной информации о событиях Великой Отечественной войны в сети, а именно создать систему автоматического поиска запрещенной информации в социальных сетях и мессенджерах, которая в режиме реального времени могла отслеживать публикации с противоправной информацией, собирая ссылки на источники данных, анализировать мнение автора публикации, классифицировав оценку по трем категориям: негативное, нейтральное и позитивное;

В-третьих, пропагандировать культуру поведения в сети Интернет, а именно составить представления о должном поведении в социальных сетях, указав на противозаконность распространения запрещенной информации в сети. В то же время просветить население, распространение какой конкретно информации запрещено на территории Российской Федерации. Например, такое положение может найти свое отражение в качестве дополнений в Федеральный Закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

Нам представляется, что указанные меры, в том числе и контроль над информацией, распространяемой в социальных сетях, позволят качественно противодействовать реабилитации нацизма и фальсификации истории Великой Отечественной войны, своевременно отвечать угрозам национальной безопасности Российской Федерации.

Список литературы

1. Куликова С. А., Кирносов И. Д. Охрана исторической памяти как институт конституционного права: российский и зарубежный опыт // Изв. Сарат. ун-та Нов. сер. Сер. Экономика. Управление. Право. 2022. № 1. С. 66–71.

2. Новый Моргенштерн: свадьба, экзистенциальный кризис и уход из шоу-бизнеса. Осторожно Собчак. URL: https://www.youtube.com/watch?v=RTVKx5okQXA (дата обращения: 06.09.2022).

3. Пестерева Ю. С., Пошелов П. В., Рагозина И. Г., Чекмезова Е. И. «Уголовно-правовая характеристика способов обмена информацией в социальных сетях на примере статей 148, 282, 354.1 УК РФ» / Вестник Томского Университета. Право, 2020. № 35. С. 112–119.

4. Приговор Пермского краевого суда от 30.06.2016 по уголовному делу № 2–17–16. URL: https://xn-90afdbaav0bd1afy6eub5d.xn – p1ai/16542187 (дата обращения: 12.09.2022).

5. Прокуратура города Москвы. Официальный сайт. Вынесен приговор по уголовному делу об оскорблении памяти ветерана Великой Отечественной войны.

URL: https://epp.genproc.gov.ru/web/proc_77/mass-media/news?item=69196006 (дата обращения: 06.09.2022).

6. СК ищет авторов видео с «элементами однополого полового акта» у Вечного огня в Александровском саду. Эхо Москвы. URL: https://echo.msk.ru/news/2930360-echo.html (дата обращения: 06.09.2022).

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.03.2022) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 30.06.2022).

8. Указ Президента Российской Федерации от 02.07.2021 № 400 “О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_389271/1e2b5c5fc29c839c457c3d876e9cc7b475bc7d45/ (дата обращения: 09.09.2022).

9. Федеральный закон от 1.07.2021 г. № 278-ФЗ «О внесении изменения в Федеральный закон «Об увековечении Победы советского народа в Великой Отечественной войне 1941–1945 годов» // СПС «КонсультантПлюс». URL: http://publication.pravo.gov.ru/Document/View/0001202107010008 (дата обращения: 30.06.2022).

10. Федеральный закон от 5 мая 2014 г. № 128-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_162575/ (дата обращения: 30.06.2022).

11. Федеральный закон от 5.04.2021 г. № 59-ФЗ «О внесении изменений в статью 354[1] Уголовного кодекса Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.kremlin.ru/acts/bank/46591 (дата обращения: 30.06.2022).

Н. Р. Шевко,
кандидат экономических наук, доцент,
Казанский филиал
Российского государственного университета правосудия

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ КИБЕРПРЕСТУПНОСТИ

Аннотация. В последнее время наблюдается резкий рост количества преступлений с использованием высоких технологий. Однако остаются нерешенными проблемы их квалификации. На основе анализа трудов известных ученых автором предложена концепция квалификации общественно опасных деяний с учетом сферы совершения. В статье приводятся статистические данные по уровню киберпреступности и затратам на защиту информационных ресурсов, а также прогнозируемые показатели противодействия киберугрозам.

Ключевые слова: киберпространство, компьютерные преступления, киберпреступления, преступления с использованием современных информационных технологий, гаджеты, информационные ресурсы, информация

PROBLEMS OF CRIMINAL LEGAL REGULATION OF CYBERCRIME

Abstract. Recently, there has been a sharp increase in the number of crimes using high technology. However, the problems of their qualification remain unresolved. Based on the analysis of the works of famous scientists, the author proposes the concept of qualifying socially dangerous acts, taking into account the scope of the commission. The article provides statistical data on the level of cybercrime and the cost of protecting information resources, as well as predicted indicators of counteracting cyber threats.

Keywords: Cyberspace, Computer crimes, Cybercrimes, Crimes using modern information technologies, Gadgets, Information resources, Information

Проблемы преступлений с использованием современных информационных технологий являются наиболее актуальными в современной юридической теории и практике. На поверхности пробелы как в теоретическом плане, так и в практическом применении уголовного законодательства в сфере противодействия компьютерным преступлениям.

С переходом всего мирового сообщества в жизнедеятельность в виртуальном пространстве, соответственно, возросла и необходимость более надежной защиты информационных ресурсов. Они отличаются от сырьевых, энергетических ресурсов рядом особенностей, а именно:

1) нематериальны, не привязаны к носителю информации, на котором представлены;

2) непотребляемы, т. е. в процессе использования они не исчезают, не утрачивают свои первоначальные свойства и т. д.;

3) не подвержены как таковому физическому износу;

4) подвержены моральному износу, причем время морального устаревания может исчисляться довольно коротким промежутком времени;

5) экономичны: их использование способствует сокращению потребления остальных ресурсов, что приводит к экономии материальных затрат;

6) не требуют дополнительных затрат для транспортировки;

7) обладают высокой скоростью передачи для дальние расстояния;

8) технически зависимы, так как их создание и использование возможно лишь с помощью компьютерной техники, причем зачастую определенного класса;

9) трансграничны;

10) обладают уязвимостью в виртуальном пространстве.

Кроме того, некоторые статистические данные заставляют серьезнее относиться к проблеме защиты информационных ресурсов. Так, согласно исследованию одного из агентств факты говорят сами за себя:

– «85 % нарушений кибербезопасности вызвано человеческим фактором;

– 94 % всех вредоносных программ доставляется по электронной почте;

– атаки программ-вымогателей происходят каждые 10 секунд;

– 71 % все кибератаки имеют финансовую мотивацию (за ними следует кража интеллектуальной собственности, а затем шпионаж)» [3].

Согласно официальной статистике, удельный вес преступлений, совершенных с помощью инновационных (в том числе и в сфере компьютерной информации), от

совокупного числа преступлений, зарегистрированных в 2021 г., составил 25,8 % [1]. Причем этот показатель с каждым годом растет. Так, согласно официальным данным Генеральной прокуратуры РФ в 2019 г. этот показатель составил 14,5 %, а в 2020 г. – 25 % (рис. 1).

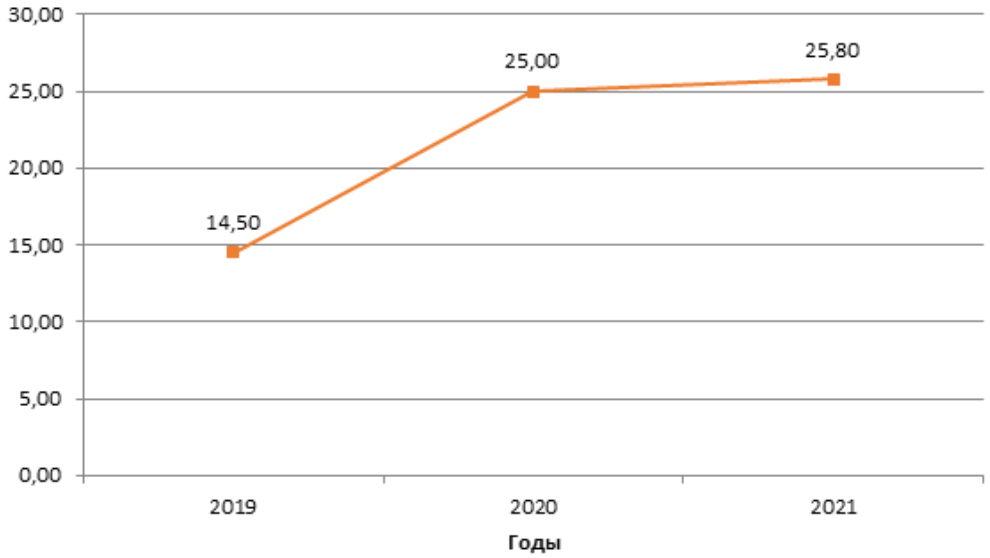

Рис. 1. Удельный вес преступлений, совершенных с использованием современных информационных технологий в РФ,%

Причем, к 2025 г. ежегодные глобальные издержки противодействия киберпреступности оцениваются в 10,5 трлн долл. [3].

Рынок кибербезопасности в 2020 г. оценивался в 176,5 млрд долл. Уже к 2027 г. прогнозируется увеличение этих сумм до $ 403 млрд. Связано это, прежде всего, с глобальной цифровизацией всего мирового сообщества, особенно в период пандемии коронавируса, когда практически все предприятия и организации были вынуждены уйти на удаленную работу, дистанционно проводить мероприятия, в то же время максимально привлекая цифровую индустрию. Именно в этих непростых условиях необходимость защиты информационных ресурсов и данных становится все более необходимой и важной.

По прогнозам специалистов, в обозримом ближайшем будущем киберпреступность будет в 5 раз прибыльнее, чем все глобальные транснациональные преступные посягательства вместе взятые. Так, наиболее распространенные и в современном мире носящие международный характер незаконный оборот наркотиков, торговля людьми, незаконная добыча и рыболовство, незаконный оборот оружия, суммарно оценивается разными агентствами от 1,6 до 2,2 трлн долл. в год [3]. В то время как обеспечение кибербезопасности к 2027 г. прогнозируется в районе $ 400 млрд.

Понятие компьютерной преступности в понимании современной теории российского уголовного права имеет более узкий смысл. В настоящее время преступления с использованием высоких технологий давно вышли за рамки чисто компьютерных преступлений. Современные телефоны фактически являются миникомпьютерами, с помощью которых также возможно совершить так называемое «компьютерное

преступление». К современным преступлениям, совершаемым с использованием высоких технологий, целесообразнее применить понятие киберпреступлений, т. е. преступлений, совершенных в киберпространстве. Тогда возникает необходимость определения киберпространства.

До недавнего времени под киберпространством понимали лишь некую «метафорическую философскую абстракцию», это было некое фантастическое понятие. Однако современность диктует свои правила и условия. Технический и технологический прогресс шагнул далеко вперед. И сейчас, наравне с отказом от понятия ЭВМ, современные условия жизни диктуют внедрение более широкого понимания компьютерных преступлений, которые стало возможно совершить не только чисто на компьютере, но и с использованием различных гаджетов, порой даже удаленно и с привязкой к адресу, находящемуся на другой стороне планеты. Ни для кого не секрет, что можно получить входящий звонок вам на сотовый телефон, условно говоря, «с вашего же номера». Причем, это самое безобидное, что можно сделать. Когда речь заходит о незаконных переводах или снятии денежных средств на приличные суммы все становится не столь безобидным. Понятно, что все это происходит не просто с помощью компьютера, и не только с помощью новых компьютерных средств, но и с использованием современных информационных технологий, причем в совершенно реальном для действий, но виртуальном для понимания пространстве, называемом киберпространством. Основным объектом киберпространства является информация – все сведения в электронном виде, в том числе персональные данные, адреса, данные банковских счетов и даже виртуальные электронные деньги.

Первые упоминания о подобном роде преступлений относятся к началу девяностых годов прошлого века, когда граждане РФ по предварительному сговору в составе преступной группы дистанционно, находясь на территории России, похитили из банка, находящегося в США, денежные средства. Ими были осуществлены десятки денежных переводов на сумму порядка 11 млн долл.

Аналогичный пример был зафиксирован на территории тогда еще СССР в 1991 г. – дело о хищении более 100 тыс. долл. и подготовке к хищению порядка $ 500 тыс.

Однако, несмотря на столь ранние упоминания о «компьютерных преступлениях» до сих пор в российской науке и практике нет четкого представления о самом этом понятии. Сложность в формулировках существует, на наш взгляд, по нескольким причинам. В первую очередь, по причине невозможности выделения единого объекта преступного посягательства, однако в любом случае инструментом является компьютерная техника с соответствующим программным обеспечением. С другой стороны, причиной является множественность предметов преступных посягательств с точки зрения их уголовно-правовой охраны. В связи с этим Ю. М. Батурин считает, что компьютерных преступлений как особой группы преступлений в юридическом смысле не существует. При этом практически все традиционные виды преступлений, за редким исключением, в части модифицировались ввиду использования для их совершения цифровой техники. Это обусловило позицию представления подобного рода преступлений не в отдельный вид, а лишь упоминание о компьютерных аспектах преступлений. Мы полностью разделяем этот подход.

Кардинально отличается мнение других ученых. Например, А. Л. Караханьян «под компьютерными преступлениями он понимает противозаконные действия, объектом или орудием совершения которых являются компьютеры». Имеются и другие точки зрения по этому вопросу. Однако мы считаем, что, к сожалению, ни одно из них в полной мере полностью не учитывает всех составляющих этого общественно опасного явления, проявляющихся в реальности.

На наш взгляд, с одной стороны, нет необходимости выделять эти преступные посягательства в отдельную категорию, поскольку фактически меняется только способ и метод совершения преступлений, не меняя сути происходящего (кража денег, мошенничество и т. д.). С другой стороны, есть необходимость определения подобного рода преступлений через понятие киберпространства, так как все они совершаются в цифровой сфере с использованием не только современных гаджетов, но и инновационных информационных технологий в виртуальном пространстве, что в большинстве своем отражается на усложнении обнаружения, расследования и пресечения противоправных действий злоумышленников. Соответственно, использование компьютерной техники при совершении преступлений необходимо рассматривать как отягчающий признак.

Преступления совершаются виртуально, а ущерб наносится вполне реальный. Примером могут служить наиболее распространенные в последнее время программы-вымогатели (разновидность фишинга) – вредоносное программное обеспечение, проникающее на компьютер пользователя и локализующий доступ к данным либо ко всему аппаратному обеспечению. Злоумышленники требуют материальный гонорар в обмен на «освобождение» (как правило, с использованием криптовалюты, поскольку трудно обнаружить получателя). Ужасает ущерб, наносимый программами-вымогателями, В год он доходит до 265 млрд долл. по всему миру, Причем явление это не редкое, в среднем одна атака происходит каждые 10 секунд. Страдают от этого как организации, так и физические лица.

Но если бы ущерб был только материальный. В 2020 г. произошла первая известная смерть в результате кибератаки, непосредственно связанной с программами-вымогателями. Тогда информационная сеть немецкой клиники в городе Дюссельдорфе подверглась кибератаке, в результате которой произошел сбой программы о наличии свободных койко-мест. В итоге жизнь женщины, вызвавшей неотложную помощь, оборвалась в связи с перенаправлением и ее госпитализацией в отдаленный филиал ввиду «компьютерной» нехватки персонала и койко-мест в ближайших клиниках в результате компьютерной атаки на компьютерную сеть.

Увеличился и срок реагирования на внедрение вредоносного программного обеспечения и противодействие ему. Если раньше антивирусные программы сами выявляли угрозы и блокировали подозрительные файлы, то в 2020 г. на обнаружение угроз информационной безопасности, как правило, занимало уже 207 дней [3].

Таким образом, киберпреступность является одним из наиболее опасных, требующих внимания и дополнительного более тщательного изучения, понятий.

Список литературы

1. Состояние преступности в России // Официальный сайт Генеральной прокуратуры РФ – Портал правовой статистики. URL: http://crimestat.ru/ (Дата обращения: 01.09.2022).

2. Шевко Н. Р., Казанцев С. Я. Кибербезопасность: проблемы и пути решения // Вестник экономической безопасности. 2020. № 5. С. 185–189.

3. 40+ статистических данных и фактов о кибербезопасности на 2022 год. URL: https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/#references (дата обращения: 10.09.2022).

В. А. Шестак,
доктор юридических наук, профессор,
Московский государственный институт международных отношений
Министерства иностранных дел Российской Федерации
П. Г. Савенкова,
соискатель магистерской степени,
Московский государственный институт международных отношений
Министерства иностранных дел Российской Федерации

РОЛЬ И ЗНАЧЕНИЕ АТРИБУЦИИ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ В ЗАРУБЕЖНЫХ СТРАНАХ

Аннотация. Масштабы правонарушений, посягающих на кибербезопасность, существенно возросли за последние годы. В результате чего стал особенно актуальным вопрос ответственности за такие правонарушения. Данное исследование посвящено анализу противоправных деяний, совершаемых в киберпространстве и посягающих на кибербезопасность. Целью данной работы является изучение процесса расследования киберпреступлений и иных противозаконных действий, а также особенностей возложения юридической ответственности на субъектов таких действий. Особое внимание уделяется институту атрибуции как этапу расследования киберпреступлений, а также отдельным аспектам его реализации в зарубежных странах.

Ключевые слова: уголовный процесс, расследование, кибербезопасность, киберпреступление, атрибуция, ответственность

ROLE AND PURPOSE OF ATTRIBUTION IN THE PROCESS OF INVESTIGATION OF CYBERCRIMES IN FOREIGN COUNTRIES

Abstract. Cybersecurity offenses have increased significantly in recent years. As a result, the issue of liability for such offenses has become particularly relevant. This study is devoted to the analysis of illegal acts committed in cyberspace and encroaching on cybersecurity. The purpose of this work is to study the process of investigation of cybercrimes and other illegal actions, as well as the peculiarities of imposing legal responsibility on the subjects of such actions. Particular attention is paid to the attribution

as a stage in the investigation of cybercrime, as well as certain aspects of its implementation in foreign countries.

Keywords: Criminal procedure, Investigation, Cybersecurity, Cybercrime, Attribution, Responsibility

Влияние киберпреступности на современное общество трудно переоценить, так, согласно статистике, приведенной Всемирным экономическим форумом, ущерб от киберпреступлений в 2021 г. составил около 6 триллионов долл. в год или 190 тыс. долл. каждую секунду [9]. В то же время вероятность обнаружения и судебного преследования лиц, ответственных за киберпреступления крайне низка и, например, в США составляет 0,05 % [2].

Ввиду того, что киберпреступность, кибератаки, киберпространство являются относительно новыми явлениями, многие положения на сегодняшний день остаются в значительной мере не урегулированными и, например, вопросы ответственности в киберпространстве являются предметом дискуссий. Поскольку любое киберпреступление непосредственно связано с компьютером и информационными системами, бóльшая часть действий преступников происходит в сети Интернет, что позволяет им оставаться анонимными и скрывать следы своей деятельности. И хотя правоохранительные органы приспосабливаются к расследованию и таких преступлений, из-за большого объема веб-данных, технической природы Интернета и информационных сетей и систем, прибегают и к менее традиционным мерам, как, например, обращение к специалистам в сфере информационной безопасности или использование искусственного интеллекта для обработки больших массивов данных. Сокрыть следы совершения преступления в Интернете значительно проще, чем в физическом мире, а вред, причиняемый такими деяниями, может многократно превышать отрицательные последствия традиционных преступлений. Для того чтобы иметь возможность применить санкции за совершение кибератак и киберпреступлений, сначала необходимо определить их происхождение, под этим понимается процесс технического, правового, политического определения индивидуальной ответственности за кибератаки. Данное действие осуществляется государствами индивидуально, каждое из которых обладает различными техническими возможностями, и действия которых основываются на различных правовых нормах, но наднациональные организации и образования осуществляют содействие. Так, например роль Европейского союза заключается в координации, сборе криминалистических данных, обмен такими данными. В значительной степени данный процесс осложнен тем, что в него могут быть вовлечены до 27 государств, в виду чего между киберинцидентом и санкциями проходит длительный период времени [4].

Вопрос юридической ответственности является одним из основополагающих как для национального, так и для международного права. Ответственность за действия в киберпространстве, несомненно, также присутствует, хотя и имеет существенные отличия от традиционного порядка. Такой институт как атрибуция повышает вероятность выявления лиц, ответственных за совершение умышленных противоправных действий в киберпространстве и позволяет привлечь

потенциальных обвиняемых к ответственности. В случае невозможности определения ответственного за киберинцидент субъекта не реализуются такие цели, как наказание стороны, ответственной за инцидент, предупреждение вредоносной активности в будущем. Способность государства проводить атрибуцию является ключевым элементом в борьбе с безнаказанностью в киберпространстве и обеспечении справедливости, как социально-правовой категории, гарантированной государством, в том числе в части обеспечения возмещения причиненного вреда для потерпевших [5].

Состояние кибербезопасности могут нарушать кибератаки или киберпреступления. Хотя в ряде случаев они используются как взаимозаменяемые, данные понятия не являются равнозначными, так, субъектом кибепреступления может быть только отдельное лицо (не государство), а также такое деяние, совершенное с помощью компьютерной системы, должно нарушать нормы уголовного закона. В то время как целью кибератаки является подрыв работы компьютерной сети и должна иметь место политическая цель ее совершения или цель нарушения национальной безопасности [8].

В отличие от кибератак, киберпреступления не подрывают компьютерную сеть, и большинство из них не преследуют политических целей или целей нарушения национальной безопасности. Хотя различие между киберпреступлением и кибератакой важно, зачастую в момент нарушения кибербезопасности не сразу становится очевидно, чем именно является то, или иное действие, так как представляется сложным сразу определить цель субъекта противоправного действия. Тем не менее, немедленное реагирование имеет первостепенное значение как в случае киберпреступления, так и кибератаки [12]. Киберпреступлением считается деяние только в том случае, если оно криминализируется в соответствии с национальным или международным законодательством. Однако правовая база, разработанная для киберсанкций, не всегда отражает технические реалии действий в информационных сетях. Критерии, которым должен соответствовать киберинцидент, чтобы оправдать юридические санкции, должны быть определены более детально. Так, в недостаточной степени проведено различие между успешными атаками и покушением. Преступное намерение и мотивацию атак редко можно установить только по техническим показателям. Тем не менее, технические индикаторы являются ключевыми для правовой оценки атаки и последующего обоснования решения о санкциях. Поэтому технические и юридические формулировки должны быть согласованы [11].

Киберпреступление негативно сказывается на потерпевшей стороне независимо от того, выступает ли в качестве таковой физическое лицо, организация или государственный орган. Выявление личности, стоящей за таким противоправным деянием имеет решающее значение для принятия мер против субъектов угрозы и предотвращения будущих эпизодов. Для правоохранительных органов установление подозреваемого в совершении киберпреступления важно для того, чтобы иметь возможность провести уголовное расследование, в то время как юридические лица больше заинтересованы в устранении ущерба и превенции. Важно отметить, что атрибуция не является самоцелью и в первую очередь должна быть

связана с более глобальной целью, которую ставит перед собой государство или группа государств, в качестве такой может выступать обеспечение кибербезопасности. В зависимости от цели процесс атрибуции может варьироваться, и могут устанавливаться различные стандарты или конкретные инструменты, доступные государству в качестве способа реагирования на такие противоправные деяния, как кибератака или киберинцидент, к которым, среди прочих, относится привлечение к уголовной ответственности [3].

Правом зарубежных стран предусматривается процесс атрибуции, под которым в широком смысле понимается определение субъекта, ответственного за совершение противоправного деяния [5]. Именно в отношении киберпреступлений данный институт имеет особое значение и, учитывая отличительные особенности таких видов преступлений, процесс атрибуции также отличается и носит название кибератрибуции. Под последним понимается процесс отслеживания, выявления и возложения вины на лицо, являющееся ответственным за совершение кибератаки или других нарушений информационной безопасности [10].

Основная сложность и неоднозначность атрибуции заключается в том, что сам процесс не относится непосредственно к уголовно-процессуальному праву или иной отрасли, а реакция на кибератаку может выражаться как в гражданском иске, так и в инициации уголовного дела, и именно надлежащее определение ответственных лиц и других особенностей каждой конкретной атаки позволяет правильно определить дальнейшие действия. Иными словами, атрибуция представляет собой предварительное условие для наложения любых дальнейших санкций.

Киберинцидент может возникнуть как в результате действий или бездействий человека, но так же и из-за внутренней неисправности компьютера. Вопрос об атрибуции возникнет лишь в том случае, если будут достаточные основания полагать, что инцидент стал результатом преднамеренного вреда. Даже в том случае, если исполнитель – физическое лицо, остается вопрос наличия вины, определение того, был ли инцидент преднамеренным, т. е. имелся ли умысел со стороны исполнителя атаки, является также одной из составляющих кибератрибуции.

Выделяют несколько подходов к определению исполнителя, ответственного за киберинцидент, которые не являются взаимоисключающими. В результате расследования можно прийти к выводу, что ответственность должна быть возложена на компьютер, физическое лицо или более широкий субъект – «ответственная сторона». Первый подход фокусируется преимущественно на технических способах определения, с помощью которых отслеживаются противоправные действия вплоть до устройства, с которого они были совершены. Анализируются методы, используемые злоумышленниками, место совершения правонарушения и иные данные, которые представляется возможным получить по результатам проведения технической экспертизы. В результате применения методов цифровой криминалистики, специалисты могут определить компьютер или устройство, с которого было совершено то, или иное деяние, однако определить лицо, находящееся в этот момент за компьютером, в подавляющем большинстве случаев не представляется возможным. Что касается второго подхода (предписывание противоправного деяния физическому лицу), под ним понимается идентификация

одного или нескольких лиц, непосредственно связанных с совершением такого противоправного деяния. Хотя в данном случае лица, проводящие расследование, также прибегают к цифровым средствам получения информации, их основной задачей является установление личности – физического лица или организации, непосредственно участвующей в реализации противоправного деяния. Так как зачастую не предусмотрено единого перечня доказательств, наличие которых будет признаваться достаточным для установления причастности того или иного лица, их количество и качество может варьироваться в зависимости от конкретной ситуации. Третий подход – определение ответственной стороны, подразумевает выявление лица или организации, имеющей умысел на совершение киберпреступления. Так, например, поднимается вопрос о возможности возложения ответственности на государство по причине того, что лицо, непосредственно выполнившее действия, составляющие противоправное деяние в киберпространсвте, является его гражданином [10].

Правовые последствия совершения противоправного деяния в киберпространстве могут в значительной степени различаться в зависимости от того, кто или что будет признано исполнителем, а также в зависимости от того, криминализовано ли деяние национальным уголовным правом и располагает ли государство достаточными доказательствами [6]. При условии, что киберпреступление криминализовано и совершено физическим лицом, оно будет регулироваться уголовным правом, однако, если последствия такого действия достаточно серьезны, чтобы поставить под угрозу национальную безопасность государства и за него несет ответственность иностранное государство, такое действие может быть рассмотрено в качестве акта агрессии и будет подпадать под регулирование международного права. Процесс определения ответственного лица осложнен также и тем, что даже в том случае, если исполнителем будет признано физическое лицо, практически невозможно установить действовало ли оно самостоятельно или от лица государства. Другое препятствие выражается в том, что государством должно быть доказано, что действия иностранного государства подпадают под категорию «вооруженного нападения», для того чтобы применялись контрмеры международно-правового характера, в противном случае, в распоряжении государства остаются исключительно уголовно-правовые и уголовно-процессуальные меры [7].

В данном контексте большое значение имеет Конвенция Совета Европы о компьютерных преступлениях (Будапештская конвенция) от 23.11.2001. В соответствии с положениями данного международно-правового договора страны-участники обязаны принять законодательные и иные меры, которые необходимы для того, чтобы деяния, предусмотренные конвенцией, квалифицировались как преступления, в соответствии с национальным уголовным правом [1]. На сегодняшний день более 60 государств включили в свои национальные законы такие преступления, как несанкционированный доступ, незаконное использование информационных систем, изменение или удаление данных и другие. Правоохранительным органам таких государств необходимо прибегать к процедуре атрибуции для того, чтобы реализовать уголовное преследование в отношении правонарушителей за вышеупомянутые деяния.

Таким образом, категория и серьезность наказания варьируются в зависимости от предмета преступления, субъектов, потерпевшего (является ли им физическое лицо или государство), и даже в случае совпадения вышеперечисленного, национальным правом государств могут быть предусмотрены различные наказания. Сложность правового регулирования кибербезопасности заключается также и в том, что существуют значительные различия между традиционными и кибер преступлениями, что влияет на необходимость разработки новых норм, а не приспособления уже существующих, а также в том, что данное явление находится на стыке нескольких областей, таких как национальное уголовное право и гражданское право, наднациональное право, право защиты персональных данных и другие. Правовая природа киберпреступлений в значительной степени отличается от традиционных, во-первых, ввиду того, что технологии развиваются с высокой скоростью, невозможно создать исчерпывающий список всех противоправных деяний, так как природа некоторых до сих пор непонятна, в отношении ряда деяний нет единого мнения о том, следует ли его криминализовать и, как следствие, считать незаконным. Во-вторых, существует большое количество обходов, как, например, реализация киберпреступлений через государство, в котором такие действия не являются уголовными преступлениями или государство, не сотрудничающее с иностранными правоохранительными органами [5]. Киберпреступления по-прежнему не имеют такого же значения, как традиционные преступления, ввиду сложности осуществления преследования и дифференциации важности, преступники продолжают активно совершать такие противоправные деяния и в большинстве случаев не претерпевают негативных последствий в виде санкций.

Список литературы

1. Конвенция Совета Европы о компьютерных преступлениях (Будапештская конвенция) от 23.11.2001. URL: https://rm.coe.int/1680081561 (дата обращения: 30.07.2022).

2. Статистика кибербезопасности: данные и анализ рынка за 2021/2022 гг. URL: https://financesonline.com/cybersecurity-statistics/ (дата обращения: 30.07.2022).

3. Banks W. Cyber Attribution and State Responsibility. International Law Studies. 2021. URL: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2980&context=ils (дата обращения: 30.07.2022).

4. Bendiek A., Schulze M. Attribution: A Major Challenge for EU Cyber Sanctions. German Institute for International and Security Affairs. 2021. December. URL: https://www.swp-berlin.org/en/publication/attribution-a-major-challenge-for-eu-cyber-sanctions#hd-d41750e3739 (дата обращения: 30.07.2022).

5. Broeders D., Busser E., Pawlak P. Three tales of attribution in cyberspace: Criminal law, international law and policy debates. The Hague Program For Cyber Norms Policy Brief. 2020. April. URL: https://securitydelta.nl/media/com_hsd/report/290/document/Three-tales-of-attribution-in-cybersopace-Hague-Program-for-Cyber-Norms-Apr-2020.pdf (дата обращения: 30.07.2022).

6. Cyber Attribution and Criminal Investigations. 2021. October. URL: https://cobwebs.com/how-cyber-attribution-plays-an-important-role-in-criminal-investigations/ (дата обращения: 30.07.2022).

7. Goel S., Nussbaum B. Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. IEEE Open Journal of the Communications Society. 2021. January. URL: https://www.researchgate.net/publication/351772839_Attribution_Across_Cyber_Attack_Types_Network_Intrusions_and_Information_Operations (дата обращения: 30.07.2022).

8. Hathaway O. The Law of Cyber-Attack. California Law Review. 2012. January. URL: http://www.jstor.org/stable/23249823 (дата обращения: 30.07.2022).

9. Hetner C., Frazzini J. How to make organizations cyber resilient in the digital frontier. The World Economic Forum. 2022. January. URL: https://www.weforum.org/agenda/2022/01/achieving-cyber-resiliency-in-today-s-digital-frontier/ (дата обращения: 30.07.2022).

10. Lin H. Attribution of Malicious Cyber Incidents: From Soup to Nuts. Columbia Journal of International Affairs. 2016. October. URL: https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents (дата обращения: 30.07.2022).

11. Shamsi J., Zeadally S., Sheikh F., Flowers A. Attribution in cyberspace: techniques and legal implications. Security and Communication Networks. 2016. October. URL: https://www.researchgate.net/publication/301705275_Attribution_in_cyberspace_techniques_and_legal_implications_SCN-SI-088 (дата обращения: 30.07.2022).

12. Yang F. The Problem With Ill-Substantiated Public Cyber Attribution: A Legal Perspective. Managing U. S.-China Tensions Over Public Cyber Attribution. 2022. March. URL: https://carnegieendowment.org/2022/03/28/problem-with-ill-substantiated-public-cyber-attribution-legal-perspective-pub-86695 (дата обращения: 30.07.2022).

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ МЕЖДУНАРОДНО-ПРАВОВЫХ ОТНОШЕНИЙ

С. А. Бурьянов,
кандидат юридических наук, доцент,
Московский городской педагогический университет
М. С. Бурьянов,
юрист, эксперт,
молодежная группа стран Содружества Независимых Государств
Международного союза электросвязи Организации Объединенных Наций

ГЛОБАЛЬНЫЕ ВЫЗОВЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ И ПЕРСПЕКТИВЫ ИХ МЕЖДУНАРОДНОГО ПРАВОВОГО УРЕГУЛИРОВАНИЯ

Аннотация. В статье рассмотрены планетарные вызовы, связанные с внедрением цифровых технологий и предложены некоторые перспективы их международного правового урегулирования. Отмечено, что, по крайней мере, некоторые из упомянутых глобальных вызовов чреваты прекращением существования человеческой цивилизации, что требует совершенствования международного правового урегулирования в целях достижения устойчивого человекоориентированного развития цифровой цивилизации. В указанном контексте предложена концепция реализации цифровых прав человека, включая возможности пользования соответствующими благами в каждой точке планеты. Обоснована необходимость принятия Декларации, а затем и Конвенции глобальных цифровых прав человека.

Ключевые слова: глобальные вызовы, цифровые технологии, международное право, цифровые права человека, устойчивое управляемое человекоориентированное развитие

GLOBAL CHALLENGES OF DIGITAL TECHNOLOGIES AND PROSPECTS FOR THEIR INTERNATIONAL LEGAL REGULATION

Abstract. The article considers the planetary challenges associated with the introduction of digital technologies and offers some prospects for their international legal regulation. It is noted that at least some of the mentioned global challenges are fraught with the cessation of the existence of human civilization, which requires the improvement of international legal regulation in order to achieve sustainable human-oriented development of digital civilization. In this context, the concept of the implementation of digital human rights, including the possibility of using the relevant benefits in every point of the planet, is proposed. The necessity of adopting the Declaration, and then the Convention of Global Digital Human Rights, is substantiated.

Keywords: Global challenges, Digital technologies, International law, Digital human rights, Sustainable human-centered development

Введение. На современном этапе ключевыми трендами развития человеческой цивилизации являются беспрецедентное усложнение и цифровая глобализация общественных, а также тесно с ними связанных природных, техногенных (и космических) взаимодействий. Глобальные вызовы непрерывно усиливаются и являются следствием, прежде всего, политико-правовых противоречий [9] в развитии глобальных процессов [4. С. 195]. Инновационные цифровые технологии стремительно развиваются и включают в себя не только персональные компьютеры и Интернет, но также: большие данные, искусственный интеллект, интернет вещей, квантовые вычисления, киберфизические системы, нанотехнологии, нейротехнологии, биотехнологии, виртуальную реальность, метавселенные и многие др. Однако их внедрение несет не только новые возможности для развития цифровой экономики, рост технологического прогресса и улучшение условий жизни людей в планетарном масштабе, но и существенные угрозы глобальной безопасности (цифровую милитаризацию, цифровое неравенство, цифровую слежку, угрозы кибербезопасности, риски сверхсильного искусственного интеллекта и др.). По крайней мере, некоторые из них чреваты прекращением существования человеческой цивилизации, что актуализирует исследование перспектив их международного правового урегулирования.

Основная часть. О состоянии изученности проблемы глобальных процессов и вызовов свидетельствуют исследования зарубежных авторов: Т. Левитта, Дж. Маклина, Р. Робертсона, Д. Медоуза, Э. Тофлера и др. Из числа отечественных ученых следует выделить Н. Н. Моисеева, В. И. Вернадского, Н. Д. Кондратьева, В. А. Карташкина, Е. А. Лукашеву, И. И. Лукашука, М. Н. Марченко, Ф. М. Рудинского, А. Н., Чумакова, А. Д. Урсула и др.

Обобщая многообразие современных подходов, отметим, что под глобализацией понимается совокупность интеграционных процессов планетарного масштаба, направленных на формирование единой взаимозависимой открытой общественно-техноприроднокосмической системы. Соответственно, глобальные вызовы – это негативные последствия возникающие вследствие неустойчивого разбалансированного развития упомянутых выше процессов. Глобалистика как относительно молодая мультимеждисциплинарная область исследований изучает глобальные процессы и вызовы, а также пути их преодоления [10]. Концепция устойчивого управляемого развития рассматривается как альтернатива нерешенности глобальных негативных последствий и прекращения развития цивилизации.

В последние десятилетия разбалансированные и не вполне урегулированные глобальные процессы претерпевают весьма масштабные и беспрецедентные трансформации [6]. В их основе лежат развитие и внедрение широкого спектра цифровых технологий нового поколения 4.0 от больших данных до искусственного интеллекта, многократно усиливающих возможности ставших привычными персональных компьютеров и сети Интернет. Например, революционное внедрение глобальных технологий 4.0 в медицине позволит вернуться к полноценной жизни или, как минимум, существенно облегчит жизнь миллионам людей с ограниченными возможностями: телемедицина; биопринтинг (трехмерная печать) необходимых органов для пересадки; нейрочипы, вживленные в мозг обездвиженных людей и позволяющие им силой мысли управлять роботизированной рукой и бытовой техникой;

нейроинтерфейсы i-BrainTech для реабилитации после инсульта; бионические глаза и импланты для восстановления слуха; бионическая кисть MeHandS от компании MaxBionic, а также иные бионические протезы на искусственном интеллекте для восстановления утраченных функций; аддитивные технологии (3D-печать) позволят индивидуализировать и удешевить упомянутые протезы. В целом медицина сможет стать более качественной и доступной в любой точке планеты, профилактика и предотвращение заболеваний выйдут на новый уровень, а внедрение роботизированных экзоскелетов позволит существенно усилить физические возможности человека. Но все же самые смелые ожидания связаны с развитием и внедрением цифровых трансплантологии, регенерации, генной терапии, превентивной медицины и прочего, что позволит существенно продлить жизнь уже в ближайшие десятилетия.

Таким образом, глобальные цифровые процессы 4.0 – совокупность планетарных интеграционных процессов, основанных на инновационных цифровых технологиях. Современные исследователи и международные организации указывают не только на небывалые возможности, вытекающие из внедрения новых цифровых технологий, но и на требующие урегулирования глобальные цифровые вызовы. Глобальные цифровые вызовы 4.0 – планетарные негативные последствия, возникающие вследствие политико-правовых противоречий внедрения упомянутых технологий, требующие объединенных усилий человечества для их преодоления в целях сохранения и устойчивого развития человеческой цивилизации [3].

Ключевым фактором формирования эволюционного перехода к устойчивому человекоориентированному развитию являются права человека [1. С. 132], закрепленные в основополагающих международных актах [5]. Наиболее весомыми являются универсальные международные документы, принятые Организацией Объединенных Наций (ООН). Так, в частности, в Уставе ООН (1945) закреплен принцип уважения прав человека. В ст. 2 Всеобщей декларации прав человека (1948) говорится, что «каждый человек должен обладать всеми правами и всеми свободами, провозглашенными настоящей Декларацией, без какого бы то ни было различия, как то: в отношении расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения». Данные положения были подтверждены в Пактах (1966) и других актах.

Ряд рекомендательных актов посвящен устойчивому развитию в условиях перехода к информационному обществу. Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» (2003) ставит своей задачей использование технологий для реализации целей Декларации тысячелетия целей развития. Важным достижением этой Декларации является рассмотрение ИКТ как инструмента, а не как самоцель развития. Так, п. 9 гласит, что «при благоприятных условиях технологии способны стать мощным инструментом повышения производительности, экономического роста, создания новых рабочих мест и расширения возможностей трудоустройства, а также повышения качества жизни для всех». Кроме того, технологии станут инструментом наведения мостов между странами и позитивного сотрудничества. В п. 12 поднимается проблема гендерного равенства касательно возможностей доступа к технологиям. Пункт 13

ставит вопрос включения в информационный мир уязвимых групп населения. Обратим внимание, что закрепляется обеспечение доступа к информации и знаниям. Поскольку каждый человек должен иметь возможность овладевать навыками и знаниями, необходимыми для понимания сущности информационного общества и базирующейся на знаниях экономики и извлечении преимуществ из этого процесса.

Полагаем, что важное значение для современной технологической повестки и для создания ориентированного на интересы человека информационного общества, которое отражено в п. 39 упомянутой Декларации, наряду с политикой технологической нейтральности, представляет принцип верховенства права. При этом п. 44 утверждает о необходимости разработки и принятия единых международных стандартов в контексте информационного общества. Информационное общество неразрывно связано с функционированием сети Интернет, так, в п. 48 говорится о необходимости многостороннего, прозрачного и демократического регулирования при полномасштабном участии органов государственного управления, частного сектора, гражданского общества и международных организаций. Данная декларация имела большое описательное значение по созданию принципов информационного общества, относящегося к Третьей промышленной революции.

В дальнейшем Планом действий Тунисского обязательства (2005) регламентирован переход от принципов к действиям с целью преодоления «цифрового разрыва» и управления пользованием Интернетом, включая обеспечение дешевого доступа и быстрого подключения. В связи с этим п. 30 обосновал Интернет как основной элемент инфраструктуры информационного общества и зафиксировал его трансформацию из научно-исследовательского и учебного инструмента в общедоступный глобальный инструмент. Существенное значение также играет обеспечение многоязычия сети Интернет, согласно п. 53. Помимо позитивной стороны, Интернет и технологии Третьей промышленной революции имеют негативный аспект: незащищенность информации личного характера, включая неприкосновенность частной жизни и данных. Так, пп. j п. 90 закладывает первые основы для разработки и внедрения приложений в области электронного правительства. Промежуточным выводом по построению информационного общества является обеспечение включения граждан в процесс развития информационного общества (предоставление доступа в Интернет) и построение его на принципах верховенства права, преодоление киберпреступности и использование ИКТ для достижения целей развития, включая преодоление нищеты.

В иных документах ООН по указанной проблематике отмечено, что цифровые технологии не существуют в вакууме – они обладают мощным потенциалом конструктивных преобразований, но также могут усилить существующие противоречия, обострить неравенство, проблемы милитаризации и нарушений прав человека. Угрозу представляют не только автономные системы оружия летального действия, искусственный интеллект также может существенно подорвать безопасность пользователей по всему миру и нашу способность самостоятельно воздействовать на окружающую действительность.

Права человека в условиях глобальной цифровой трансформации постоянно находятся в фокусе внимания Организации Объединенных Наций (ООН) и ее специализированных учреждений [11]. Данная проблематика отражена в программ-

ном докладе Генерального секретаря ООН А. Гуттериша «Наша общая повестка дня» [16].

Всемирный социальный доклад за 2021 г., как основная публикация Департамента по экономическим и социальным вопросам Организации Объединенных Наций (ДЭСВ ООН), посвящен проблемам ускорения социально-экономического роста и борьбе с изменением климата в разгар восстановления после COVID-19. В частности, в докладе предложены новые стратегии с акцентом на использование новых цифровых технологий [15].

В конце марта 2022 г. Генеральный секретарь Организации Объединенных Наций А. Гутерриш в своем «Докладе о миростроительстве и поддержании мира» подчеркнул, что современный мир подвержен максимальному числу военных конфликтов с 1945 г., где жертвами насилия и нарушений прав человека является четвертая часть человечества, т. е. около 2 млрд человек. «Это происходит во время возрастающих рисков, которые делают мирное сосуществование еще более недосягаемым, – таких как экономическое неравенство, COVID-19, изменение климата и киберугрозы», – сказал Гутерриш [13].

В этих сложных условиях неравномерной цифровой трансформации ООН прилагает усилия для формирования открытого, свободного и безопасного цифрового будущего для всех через: подтверждение фундаментальной приверженности подключению неподключенных; избежание фрагментации Интернета; предоставление людям вариантов использования их данных; применение прав человека в Интернете; и содействие созданию надежного Интернета.

Современные глобальные вызовы нашли отражение в дискуссиях Давосского форума, прошедшего с 17 по 21 января 2022 г. также при активном участии ООН. В повестке форума были следующие вопросы: климатические действия (неудачные меры по борьбе с изменением климата, экстремальные погодные явления и утрата биоразнообразия, достижение нулевых углеродных выбросов, переход к чистой безуглеродной энергетике, экономика замкнутого цикла и устойчивое потребление, восстановление природы); проблемы восстановления после пандемии COVID-19 (борьба с устойчивостью вируса к противомикробным препаратам, различия в охвате услугами здравоохранения, важность охраны психического здоровья для всех); экономическая и социальная устойчивость (борьба с бедностью и неравенством доходов, программы социальных расходов, рост цен на продукты питания и энергию, стабилизация и устойчивость экономики, проблемы справедливости в отношении вакцин, социальная мобильность, рабочие места и равные возможности для всех); глобальное сотрудничество (проблемы доверия к институтам, распространение ложной информации и дезинформации, цифровая трансформация бизнеса и общества, безопасность продуктов питания, помощь малым предприятиям и предпринимателям); вызовы цифровизации (киберпреступность, увеличение цифрового разрыва, баланс инноваций и ответственности) [14].

В частности, Программа развития Организации Объединенных Наций (ПРООН) охватывает большинство государств и выступает координатором в деле достижения устойчивого глобального и внутригосударственного развития через поддержку прав человека, доступ к знаниям и опыту [16].

Заключение. Права человека являются одним из ключевых приоритетов современного международного права [8. С. 40]. В Конституции России права человека закреплены в качестве высшей ценности и одной из основ строя. Цифровая трансформация глобального общества требует существенного развития международного права, основанного на правах человека. В целях научной разработки и международно-правового закрепления глобальных цифровых прав человека на базе Global Law Forum было сформировано сетевое сообщество и исследовано влияние цифровой фазы глобальных процессов 4.0 на права человека в контексте достижения целей ООН в области устойчивого развития. В рамках проекта Global Digital Human Rights for 4IR, инициированного Global Shapers Community Moscow (WEF) в партнерстве с Global Law Forum был разработан инструментарий для анализа и оценки необходимости правового закрепления цифровых прав человека в международном праве и внутригосударственных правовых системах. При участии Global Shapers Community, an initiative by the World Economic Forum со всего мира был проведен опрос, который выявил необходимость разработки, принятия и реализации Декларации глобальных цифровых прав человека в качестве важного инструмента противодействия глобальным цифровым угрозам. Опрос показал, что 98 % респондентов из различных стран мира (Австралия, Аргентина, Бруней, Бразилия, Великобритания, Германия, Греция, Камерун, Мексика, Мали, Россия, Швейцария, США и др.) считают, что принятие и реализация Декларации глобальных цифровых прав человека может создать условия для ориентированного на каждого человека направления развития 4IR и преодоления глобальных угроз (цифрового неравенства, цифровых войн, цифровых диктатур и др.). Кроме того, продвижение идеи новых глобальных цифровых прав человека было осуществлено на научных конференциях и молодежных форумах, вовлекая заинтересованные стороны в решение данных вопросов, в том числе через сообщества Интернет. Концепция глобальных цифровых прав человека была представлена и стала победителем на форуме «Формируем будущее вместе» и конкурсе «Горизонт-2100», проведенных при поддержке ООН [7]. Также данная концепция была поддержана молодежными послами ЦУР ООН СНГ в ходе круглого стола по Целям устойчивого развития Основной группы ООН по делам детей и молодежи (UN MGCY), состоявшегося на полях Политического форума высокого уровня по устойчивому развитию ООН (HLPF). Летом 2020 г. М. С. Бурьяновым был разработан проект Декларации глобальных цифровых прав человека, а в повестке дня World Economic Forum опубликована статья в ее поддержку [12].

В качестве вывода отметим, что правовое закрепление и реализация цифровых прав человека 4.0 является ключевым фактором устойчивого управляемого человекоориентированного развития общества в условиях современных глобальных технологических и социально-экономических трансформаций. На универсальном международном уровне в рамках Организации Объединенных Наций представляется целесообразным принятие Декларации, а затем и Конвенции глобальных цифровых прав человека [2]. Далее имплементация на внутригосударственных уровнях призвана создать условия для осуществления цифровых прав и возможности пользования общественно-технопродными и космическими благами в каждой точке планеты. После Второй мировой войны принятие Устава ООН 1945 г., Всеобщей

декларации прав человека 1948 г. и иных основополагающих актов в области прав человека стало основой перехода к новой эпохе правового регулирования в интересах устойчивого развития мирового сообщества. Сегодня, в условиях цифровой глобализации, необходимо кардинальное обновление международных обязательств в области прав человека в направлении закрепления и реализации доступа каждого к новым технологиям 4.0.

Список литературы

1. Бурьянов М. С. Значение права в условиях современных глобальных процессов // Актуальные проблемы становления и развития правовой системы Российской Федерации: сборник материалов II Всероссийской научно-практической конференции студентов, магистрантов и аспирантов (г. Сыктывкар, 5–6 апреля 2018 г.). Сыктывкар: Изд-во СГУ им. Питирима Сорокина, 2018. С. 130–133.

2. Бурьянов М. С. Цифровые права человека в условиях глобальных процессов: теория и практика реализации: монография / М. С. Бурьянов; под науч. ред. С. А. Бурьянова. Москва: РУСАЙНС, 2022.

3. Бурьянов С. А., Бурьянов М. С. Новые угрозы глобальной безопасности и перспективы развития международного права // Евразийский юридический журнал. 2020. № 11 (150). С. 35–40.

4. Бурьянов С. А., Кривенький А. И. О состоянии и перспективах формирования глобального образования, включая юридическое // Государство и право. 2019. № 8. С. 95–100.

5. Епифанов А. Е., Лакеев А. Е. Действие международно-правовых стандартов в правовой системе Российской Федерации: монография. Москва: Юрлитинформ, 2014.

6. Лукашук И. И. Глобализация, государство, XXI век. Москва, 2000.

7. Международный проект «ГОРИЗОНТ 2100»: молодежный форум «Формируем будущее вместе». URL: https://www.youtube.com/watch?v=1697m-GEWQ4 (дата обращения: 21.07.2022).

8. Николаев А. М., Давтян М. К. Исполнение решений Европейского Суда по правам человека и Межамериканского Суда по правам человека: сравнительный анализ // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 4 (71). С. 40–46.

9. Фархутдинов И. З. Американская доктрина о превентивном ударе от Монро до Трампа: международно-правовые аспекты. Москва, 2018.

10. Чумаков А. Н. Глобальный мир: столкновение интересов: монография. Москва, 2018.

11. Abashidze A., Kiseleva E., Ilyashevich M., Nikolaev A., Belousova A. The right to education of vulnerable groups of children in the Russian Federation in the light of the activities of the un committee on the rights of the child // Journal of Advanced Research in Law and Economics. 2018. Т. 9, № 3. С. 792–804.

12. Burianov M. Here's why we need a Declaration of Global Digital Human Rights // World Economic Forum. URL: https://www.weforum.org/agenda/2020/08/here-s-why-we-need-a-declaration-of-global-digital-human-rights/ (дата обращения: 21.07.2022).

13. Secretary General on the war in Ukraine: “a catastrophe that shakes the foundations of the world order”. URL: https://news.un.org/ru/story/2022/03/1420992 (дата обращения: 21.07.2022).

14. The Davos Agenda 2022 brings together world leaders to address the state of the world. URL: https://www.weforum.org/agenda/2022/01/the-davos-agenda-2022-addressing-the-state-of-the-world/ (дата обращения: 21.01 2022).

15. UNDESA World Social Report 2021. URL: https://www.un.org/development/desa/dspd/world-social-report/2021–2.html (дата обращения: 21.07.2022).

16. United Nations Secretary-Generals Report «Our common agenda». URL: https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf (дата обращения: 21.07.2022).

Е. Е. Гуляева,
кандидат юридических наук, доцент,
Дипломатическая академия Министерства иностранных дел
Российской Федерации

МЕЖДУНАРОДНО-ПРАВОВАЯ КОНЦЕПЦИЯ ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. Настоящая статья посвящена международно-правовой концепции применения информационно-коммуникационных систем и цифровых технологий. Автор рассматривает понятия «информационные права», выделяет два основных юридических подхода к регулированию системы обеспечения международной безопасности: фрагментарный и комплексный. Автор статьи приходит к выводу, что разрыв в техническом обеспечении предполагает существование условно информационно «богатых» и информационно «бедных» государств, что, по сути, негативно влияет на соблюдение принципа суверенного равенства государств в международном праве.

Ключевые слова: право, правовая доктрина, информационные коммуникационные технологии, цифровые технологии, международное сотрудничество, принципы международного права

INTERNATIONAL LEGAL CONCEPT OF THE APPLICATION OF INFORMATION COMMUNICATION SYSTEMS AND DIGITAL TECHNOLOGIES

Abstract. This article is devoted to the international legal concept of the use of information and communication systems and digital technologies. The author considers the concept of «information rights», identifies two main legal approaches to the regulation of the system of ensuring international security: fragmented and complex. The author of the article comes to the conclusion that the gap in technical support implies the existence of conditionally informationally “rich” and informationally “poor” states, which in

fact negatively affects the observance of the principle of sovereign equality of states in international law.

Keywords: Law, Legal concept, Information communication systems, Digital technologies, International cooperation, Principles of international law

В настоящее время довольно сложно предположить, каким образом будет развиваться международное сотрудничество государств в сфере применения информационных телекоммуникационных систем и цифровых технологий для поддержания международного мира и безопасности. Очевидно, что перед государствами всего мира остро встает вопрос о поиске новых путей, парадигм разрешения проблемы обеспечения международной и, как следствие, глобальной безопасности. При этом традиционные методы решения проблемы уже не являются достаточными. Возникает вопрос о возможности применения современных информационных технологий, а также иных достижений науки и техники для обеспечения международной безопасности. Рассмотрение поставленного вопроса с указанных позиций ставит перед научным сообществом множество вопросов: какие технологии могут быть использованы, их пределы, варианты правового регулирования, соотношение практики использования указанных технологий с общепризнанными принципами и нормами международного права и т. д.

Зачастую мы видим попытки управления информационным пространством на государственном уровне с целью манипулирования общественным мнением и преподнесением информации о вопросах (так называемый феномен фэйк-ньюс), затрагивающих международную безопасность в том ключе, который выгоден конкретной политической элите.

В результате потребуется дальнейшее совершенствование нормативно-правового регулирования порядка оказания трансграничных услуг информационными компаниями, являющимися национальными юридическими лицами конкретных государств, например, таких, как Google, Facebook (признана экстремистской организацией, запрещена в РФ), Amazon, Яндекс и т. п.

Составным элементом международной безопасности является также безопасность личности, которая в новых, глобализирующихся условиях принимает вид обеспечения защищенности граждан в информационном пространстве (обеспечение информационных прав). Информационные права граждан признаются и закрепляются не только на национальном, но и на международном уровнях. Поэтому лица, с учетом установленных ограничений, могут реализовывать свои информационные права на территории других государств, что является существенной предпосылкой для международного информационного обмена.

В рамках теоретической проработки вопросов о правах человека в сфере информационного обмена появилась концепция *права человека на коммуникацию*, создатели которой пришли к выводу, что в международном праве на момент разработки концепции отсутствовал единый принцип, на основании которого осуществлялось бы управление вопросами коммуникации в масштабе всей планеты. Поэтому экспертами было предложено включить в международно-правые акты *право человека на уникальную коммуникацию* [1. С. 127–135].

Одной из составных частей права на информацию является право граждан на получение информации о деятельности органов государственной власти. В ходе реализации данного права современные государства не могут сокрыть информацию, которая имеет жизненно важное значение для большого числа граждан. В определенных случаях высказывается мнение об установлении приоритета соответствующего информационного права гражданина над интересами национальной безопасности.

Актуальным в современных условиях является вопрос об обеспечении сохранности персональных данных граждан в условиях формирования информационного общества. Данный аспект права стал чуть ли не важнейшим видом обеспечения прав граждан в последние десятилетия. Так, основополагающим нормативно-правовым актом в сфере прав человека провозглашено право на неприкосновенность частной жизни, которое, однако, может быть ограничено в связи с активной информатизацией общественных отношений.

Стоит отметить, что в связи со сложной эпидемиологической ситуацией в мире из-за распространяющейся коронавирусной инфекции (COVID-19) информационные права граждан отдельно взятого государства претерпевают существенные изменения: нередки случаи, когда вопрос обеспечения национальной безопасности стоит выше любого другого права индивида или отдельно взятой группы лиц.

Другим важным и актуальным аспектом является доступ, использование и применение информации в огромных информационных массивах (Big Data), т. е. такой технологии, когда сведения о гражданах, в том числе составляющие их персонифицированные данные, сосредотачиваются в одном месте и могут использоваться для различных целей. Все это создает не только угрозу нарушения информационных прав граждан, но и увеличивает риск компрометации этих данных.

Принято считать, что развивающиеся стремительными темпами глобальные информационно-коммуникационные технологии оказывают исключительно благоприятное воздействие на человека и общественные отношения. В частности, указывается на огромное расширение возможностей по обмену информацией, по поддержанию социальных связей, по развитию глобальной экономики [2. С. 295]. Именно развитием указанных технологий определяется качественный переход человечества в информационное общество (new information era). Но нельзя забывать о том, что современные коммуникационные технологии, помимо очевидного позитивного эффекта, могут стать источником нарушения состояния защищенности общества или его отдельных элементов.

Современные тренды развития информатизации могут представлять определенную угрозу в случае неконтролируемого развития соответствующего сегмента информационного пространства. Попробуем проследить данные тенденции на примере развития международной глобальной сети Интернет, систем искусственного интеллекта и Big Data.

Существенным моментом в направлении развития правового механизма регулирования использования сети Интернет и обеспечения безопасности стало принятие Лондонского плана действий по международному сотрудничеству в области применения законодательства против спама [3. С. 48–51]. В указанном документе

прослеживается дальнейшее развитие положений, содержащихся в Меморандуме о взаимопомощи в вопросах коммерческих рассылок по электронной почте, составленном Федеральной торговой комиссией США, Офисом по законной торговле Великобритании, Уполномоченным по информации и некоторыми другими уполномоченными органами ряда зарубежных стран. Россия также присоединилась к указанному плану действий.

Попыткой урегулирования на международном уровне отношений в части использования сети Интернет и минимизации связанных с этим риском стало принятие программы ЮНЕСКО «Информация для всех». Названный документ призван оказать содействие в выработке единого глобального подхода к этическим и правовым нормам, регулирующим информационное пространство. Проблематика нежелательных информационных сообщений (спама) стала предметом обсуждения на Всемирном саммите по информационному обществу. По результатам проведения данного мероприятия была принята Тунисская программа для информационного общества [4. С. 539], в соответствии с которой должны быть приняты эффективные меры для скорейшего разрешения проблемы спама.

В соответствии с резолюцией Генеральной Ассамблеи ООН A/RES/33/115 от 18.12.1978 «Вопросы, касающиеся информации» закрепляется принцип свободного, широкого и сбалансированного распространения информации. Правовое регулирование распространения информации посредством сети Интернет основывается на базовых принципах, которых предоставляют любому государству возможность создания на своей территории компьютерных сетей и гарантируют возможность участия государств в международном информационном обмене. С другой стороны, констатируется, что каждое государство имеет право на принятие мер защиты от вредной и общественно опасной информации. Соответствующие тезисы нашли свое закрепление в Конвенции Совета Европы «О киберпреступности».

Интересно отметить, что Россия отказалась подписать данный документ. Одним из ключевых положений Конвенции является предоставление доступа государствами к собственным техническим средствам другим участникам Конвенции.

В настоящее время в международной практике правового регулирования распространения информации в сети Интернет сложилось три основных модели, которые стали реакцией международного сообщества и национальных государств на те угрозы, которые исходят от сети Интернет, в частности от неконтролируемого распространения вредоносной информации.

Первая модель заключается в установлении полного контроля государства за распространением информации в сети Интернет. Наиболее ярким примером такой модели является Китай. В соответствии с законом КНР «О телекоммуникациях» для начала своей деятельности интернет-провайдеры обязаны получить лицензию в уполномоченном органе государственной власти с раскрытием основных параметров своей компании. Кроме того, интернет-провайдеры должны хранить информацию о своих сайтах, их посещениях и предоставлять данную информацию сотрудникам правоохранительных органов [7. С. 488–497].

Согласно второй модели, интернет-провайдеры несут ответственность за любые действия пользователя. Так, в соответствии с французским законодатель-

ством они обязаны сообщать информацию о владельцах сайтов и авторах контента на них любым заинтересованным лицам, в противном случае они рискуют быть привлеченными к уголовной ответственности. Пример Франции интересен также тем, что еще в 1978 г. была создана Национальная комиссия информатики и свобод, которая была уполномочена на осуществление контрольных мероприятий в сфере информатизации [8. С. 15–23].

В соответствии с третьей моделью правового регулирования распространения информации в сети интернет-провайдеры освобождаются от несения ответственности при условии, что они выполнили предусмотренные законодательством действия в части предоставления услуг и взаимодействия с пользователями. Например, в соответствии с немецким законодательством интернет-провайдеры не могут нести ответственность за размещение противоправной информации только в том случае, если они являются непосредственными распространителями данной информации или ее собственниками. При этом у провайдеров отсутствует обязанность удалять незаконную информацию, которая была размещена на их серверах.

Искусственный интеллект принято делить на слабый и сильный. Сильный искусственный интеллект характеризуется наибольшей приближенностью к параметрам человеческого разума, что предполагает возможность обработки им чувственной информации. К настоящему времени еще не удалось создать киберфизическую систему общего назначения, но стоит ожидать возможное решение данной задачи в ближайшее время. Поэтому очень важным является формирование соответствующей нормативной базы использования искусственного интеллекта в форме роботов, для чего необходимо выделить приоритетные направления, по которым должно осуществляться правовое регулирование как на национальном, так и на международном уровнях:

1) проведение стандартизации систем искусственного интеллекта;

2) проведение лицензирования деятельности, связанной с созданием и использованием систем искусственного интеллекта;

3) обеспечение конфиденциальности персональных данных;

4) соблюдение норм профессиональной этики.

В настоящее время искусственный интеллект, обучаемый на базе глубоких нейронных сетей, повсеместно применяется специалистами и учеными в различных областях: в прогнозировании, в системах массового обслуживания, в анализе данных и др. Особую популярность набирает направление создания и использования беспилотных летательных и транспортных средств на базе искусственного интеллекта.

Традиционно новеллы правового регулирования, прежде чем стать предметом регулирования международно-правовых актов, принимаются на уровне национальных государств. Если говорить о сфере искусственного интеллекта, и в частности робототехники, то первым государством в мире, в котором были на официальном государственном уровне утверждены правила передвижения курьеров-роботов, стала Эстония. В Германии действует закон, в соответствии с которым вводятся более простые правила относительно перемещений транспортных средств, управляемых искусственным интеллектом. Но при этом для владельцев такого транспорта установлены повышенные санкции за допущенные нарушения. При этом ответственность

за любые происшествия с транспортным средством все равно несет водитель, т. е. участие человека во время управления транспортным средством признается обязательным [9. С. 99–102].

В Японии несколько лет назад были разработаны законы, посвященные осуществлению контроля за использованием систем искусственного интеллекта. В указанных документах в первую очередь решаются вопросы, связанные с авторским правом на технологии искусственного интеллекта. В соответствии с японским законодательством авторские права на указанные технологии принадлежат заказчикам, но в последующем предполагается осуществление перехода исключительных прав к разработчикам. Также интересной особенностью японского законодательства является возложение на компании-разработчики систем искусственного интеллекта ответственности за возникновение любых негативных последствий от использования искусственного интеллекта, в том числе возмещение ущерба пострадавшим лицам.

Стоит отметить, что Япония уже сравнительно длительное время предпринимает попытки по разработке наиболее оптимальных способов регулирования рынка искусственного интеллекта. Планируется введение сертификатов соответствия требованиям безопасности для робототехники [10. С. 117–124].

Важно отметить и тот факт, что новые технологии могут нести определенный риск для жизни и здоровья граждан – проведение DDoS-атак на важные объекты инфраструктуры, создание фейковых новостей на базе искусственного интеллекта или даже обычное использование беспилотных транспортных средств. Распространение же антиправительственной информации через скрытые сетевые ресурсы сети Интернет несет непосредственную угрозу для конституционной целостности государства и поддержания общественного порядка.

Наличие у государства информационного оружия дает ему преимущества перед другими государствами, у которых такого оружия нет. Все это ставит проблему так называемого цифрового разрыва, когда существует неравенство государств в распределении научно-технологических ресурсов и доступа к информационным технологиям. Этот разрыв предполагает существование условно информационно «богатых» и информационно «бедных» государств [11. С. 70–74].

Информация стала источником появления новых проблем по причине слишком активного развития информационных технологий. Появление высокоточного оружия, оружия массового уничтожения и вооружений, основанных на новых физических принципах, создает непосредственную угрозу для существования всего человечества. Ведение войны традиционными способами и средствами не идет ни в какое сравнение с современными видами вооружения и последними достижениями научно-технического прогресса.

Современные конфликты между государствами все чаще переходят из ведения боевых действий на земле в информационное пространство. В результате воюющие стороны стали активно использовать информационно-коммуникационные технологии для причинения ущерба другим государствам, что противоречит правилам и нормам международного общения.

Деятельность, связанная с обеспечением международной информационной безопасности, является одним из актуальных направлений международного со-

трудничества государств по вопросам обеспечения и поддержания международной безопасности в целом. К настоящему времени сложились два основных юридических подхода к регулированию системы обеспечения международной безопасности: фрагментарный и комплексный.

Данные подходы образуют основу современных концепций обеспечения информационной безопасности на различных уровнях регулирования. Изучая содержание этих подходов, можно установить основные положения соответствующих концепций. В отличие от содержания нормативно-правовых актов международного уровня по вопросам обеспечения безопасности, правовые концепции являются стабильными и мало изменчивыми. Они определяют базовые позиции государств по вопросам международной безопасности [12. С. 124–135].

Кроме того, для всех моделей концепций международной информационной безопасности характерно наличие общей цели, а именно формирование международной кибербезопасности.

Общепризнано, что государство на международной арене должно своими усилиями способствовать социальному и экономическому развитию общества. При этом соответствующая деятельность государств должна соотноситься с идеями поддержания мира и международной безопасности, неприкосновенности суверенитета государств и защиты прав и свобод человека и гражданина. Также важны принципы международной информационной безопасности. Например, государства в ходе осуществления своей информационной деятельности должны принимать во внимание принцип неделимости безопасности, принцип ответственности за находящееся в их юрисдикции информационное пространство. Неделимость безопасности означает, что для обеспечения национальной безопасности государства имеет значение состояние защищенности всех основных сфер жизни общества у других государств и всего мирового сообщества в целом.

В соответствии с постулатами первой концепции, которая получила название фрагментарной, современная международная информационная безопасность направлена в первую очередь на противодействие совершению уголовных преступлений в сфере высоких технологий. Именно данный аспект нуждается в правовом регулировании нормами международного права. Но в неразрывной связи с указанным аспектом находится и такая задача правового регулирования, как противодействие террористической деятельности, совершаемой посредством информационно-коммуникационных технологий и реализуемой непосредственно в информационном пространстве [13. С. 71–75].

Вторая концепция именуется комплексной. В соответствии с ее идеями требуется широкое освещение проблематики в сфере международной информационной безопасности. Сторонники названной концепции считают, что международная безопасность является неделимой, поэтому государства должны обеспечивать комплексный подход к вопросу обеспечения национальной и международной безопасности в целом, не акцентируя внимания исключительно на вопросах информационной безопасности.

Исходя из названия концепции, использование информационно-коммуникационных технологий для предотвращения военных, террористических и преступных

угроз должно реализовываться комплексно. Вследствие этой базовой идеи, соответствующее международно-правовое регулирование должно распространяться на все составные части международной информационной безопасности.

Проблемным вопросом в данной доктрине является необходимость осуществления правового регулирования как составной части международной информационной безопасности. Известно, что международно-правовое регулирование может иметь как информационное, так и коммуникационное направление. С точки зрения международного права, названные направления принято рассматривать с позиций недопущения использования информационно-коммуникационных технологий в двух случаях:

– при причинении ущерба правам и законным интересам граждан;

– при причинении ущерба основополагающим частям государства.

Наиболее общим проявлением вышеперечисленных негативных действий является трансграничное распространение информации при помощи информационно-коммуникационных технологий. Причем речь идет об информации, содержание которой вступает в противоречие с принципами и нормами международного права. Также не исключено, что негативными проявлениями незаконных действий станет использование информационных сетей государств для распространения запрещенной информации.

Говоря о техническом направлении, соответствующее противодействие направлено на причинение вреда различным структурным элементам государства (например, финансовой, политической и другим сферам).

Представители фрагментарной концепции вообще не рассматривают вопрос о регулировании и соотношении содержательного и технического элементов международной информационной безопасности. Сторонники фрагментарной концепции полагают, что достаточными являются нормы Конвенции о киберпреступности с соответствующими дополнительными протоколами. В соответствии с положениями комплексной концепции допускается возможность правового регулирования одновременно функциональных и структурных элементов международной информационной безопасности. В качестве примера такого типа регулирования можно привести Соглашение между правительствами государств – членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности, подписанное в 2009 г.

Особое внимание стоит обратить и на тот факт, что еще в 80-е гг. XX в. предлагались концепции, в соответствии с которыми должна быть сформирована единая концепция международной безопасности без видового разделения. Эта концепция являлась, прежде всего, документом политического характера с соответствующим инструментарием, но специалистами она все же увязывалась с международным правом [15. С. 77–80]. Довольно популярным является мнение о том, что нормы в сфере международной информационной безопасности должны получить развитие в контексте обеспечения полной системы международной безопасности [16. С. 30–35]. В подтверждение обоснованности предложенного взгляда на решение проблемы, можно привести принятую Генеральной Ассамблеей ООН резолюцию № 41/92 «О создании всеобъемлющей системы международно-

го мира и безопасности». В ходе обсуждения содержания указанного документа выдвигались предложения о создании Всемирной программы обеспечения мира и безопасности на планете.

Следует заметить, что указанные концепции не являются устойчивыми. Причинами этого является деятельность отдельных государств, направленная на разработку средств информационного подавления и ведения информационных войн. С другой стороны, большинство государств заинтересованы и предпринимают соответствующие действия для выработки наиболее оптимальных подходов к регулированию проблем международной информационной безопасности.

Ведущая роль в координации усилий международного сообщества по обеспечению международной информационной безопасности принадлежит ООН, деятельность которой преимущественно направлена на создание нормативно-правовой базы противодействия совершению преступных деяний при помощи информационно-коммуникационных технологий, но не предусматривает при этом механизма превентивных действий для купирования подобной угрозы еще на стадии планирования и проектирования. На международном уровне нет общепризнанного списка запрещенных для посещения сетевых ресурсов, доступ к которым должен быть заблокирован на национальном и региональном уровне с учетом интересов региональных стратегических партнеров – поставщиков информации в глобальной сети Интернет.

Возвращаясь к вопросу о концепциях регулирования системы обеспечения международной безопасности по части вопросов информационной безопасности, резюмируем, что исторически сложились две основные противоборствующие концепции. Наиболее предпочтительной является комплексная концепция, так как проблематика обеспечения международной безопасности в современных условиях не может не учитывать всю совокупность негативных факторов, действующих на состояние защищенности основных сфер жизнедеятельности общества. Более того, недопустимо игнорировать и другие возрастающие риски для международной безопасности в целом. Однако, учитывая скорость распространения информации и потенциальный ущерб, к которому может привести дезинформация о важных событиях в стране или регионе, акцент стоит делать именно на информационную безопасность как компонент регулирования международной безопасности.

Важно отметить, что использование злоумышленниками современных технологий для совершения противоправных деяний в киберпространстве не проходит бесследно и предполагает оставление цифровых следов их деятельности. То есть существует принципиальная возможность использования новейших технологий для раскрытия и расследования подобных преступлений. Такие возможности составляют основу соответствующего международно-правового регулирования в сфере информационной безопасности.

Как следует из вышесказанного, отдельные государства и международное сообщество в целом едины в понимании того факта, что сеть Интернет предоставляет не только определенные преимущества, но и вызывает к жизни существенные проблемы, которые необходимо решать. К таким проблемам относится, в частности,

обеспечение глобальной информационной безопасности, защита персональных данных, вопросы юрисдикции и идентификация пользователей.

Список литературы

1. Павлов В. И. Идеи правовой коммуникации и современная антропология права // Известия высших учебных заведений. Правоведение. 2014. № 5. С. 127–135.

2. Инновационные направления современных международных отношений: учебное пособие для студентов вузов / под ред. А. В. Крутских, А. В. Бирюкова. Москва: Аспект Пресс, 2010. 295 с.

3. Михайлусов С. Н. Международно-правовое регулирование Интернета // Право и управление. XXI век. 2010. № 2. С. 48–51.

4. Касенова М. Б. Институциональная структура и нормативно-правовые основы трансграничного управления интернетом: дис. … д-ра. юрид. наук. Москва, 2014. 539 с.

5. Вопросы, касающиеся информации: резолюция ГА ООН от 18.12.1978. URL: https://undocs.org/ru/A/RES/33/115 (дата обращения: 16.09.2022).

6. Конвенция о преступности в сфере компьютерной информации (ETS N 185) (заключена в Будапеште 23.11.2001) // СПС «Консультант-плюс».

7. Трощинский П. В. Особенности правового регулирования безопасности сети Интернет Китая // Журнал зарубежного законодательства и сравнительного правоведения. 2014. № 3. С. 488–497.

8. Иванова К. А., Степанов А. А. Ограничения свободы слова во Франции в эпоху цифровых технологий // Правоприменение. 2019. № 1. С. 15–23.

9. Лавриненко А. В. К вопросу о правовом регулировании использования беспилотных транспортных средств // Юридическая наука в XXI веке: сборник научных статей по итогам работы круглого стола. 2018. С. 99–102.

10. Чучаев А. И., Маликов С. В. Ответственность за причинение ущерба высокоавтоматизированным транспортным средством: состояние и перспективы // Актуальные проблемы российского права. 2019. № 6. С. 117–124.

11. Нежельский А. А. Теоретические основы исследования информационных войн и информационной безопасности государства // Власть. 2018. № 6. С. 70–74.

12. Дюкарев В. В. Современные проблемы и концепции международной безопасности // Вопросы права и политики. 2011. С. 124–135.

13. Ибрагимов Л. Х. Интернет-терроризм как феномен современных политических коммуникаций // Информационные войны. 2016. № 2. С. 71–75.

14. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (заключено в г. Екатеринбурге 16.06.2009) // СПС «Консультант-плюс».

15. Лисаускайте В. В. Проблемы реформирования концепции международной безопасности в международном публичном праве // Безопасность XXI века: материалы конференции. 2001. С. 77–80.

16. Кочетков В. В. Изменения в подходах к международной безопасности в начале XXI века // Вестник Московского университета. Серия 12: Политические науки. 2010. № 4. С. 30–35.

17. Резолюция Генеральной Ассамблеи ООН № 41/92 от 04.12.1986 «О создании всеобъемлющей системы международного мира и безопасности». URL: https://undocs.org/ru/A/RES/41/92 (дата обращения: 16.09.2022).

18. Положения Всемирной программы обеспечения мира и безопасности на планете. URL: https://www.un.org/ru/sections/issues-depth/peace-and-security/index.html (дата обращения: 16.09.2022).

Е. В. Дятлова,
старший преподаватель,
Казанский инновационный университет имени В. Г. Тимирясова

ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Аннотация. В статье рассматривается техническая архитектура Интернета, которая определяет содержание институтов и субъектов, вовлеченных в правовые отношения в Интернете, и необходимость правового надзора за их использованием, выявляется основополагающее значение на национальном и международном уровне,поспособствовавшее развитию многих форм управления Интернетом, для которых основным принципом является участие всех сторон. Поскольку интернет – это многоуровневая сеть технической информации, можно сказать о том, что ее деятельность осуществляется в установленных пределах. При этом невозможно точно определить объект и субъект управления правоотношениями, связанными с использованием Интернета. Вышеупомянутые правовые отношения по контролю за сетью, распространяются на программное и аппаратное обеспечение для подключения различных частей сети передачи данных в разных странах, включая систему корневых серверов, которая направляет основной поток данных в Интернете, каналы и оборудование физического соединения, технические стандарты и методы фактической реализации сетевых адресов устройства связи и многое другое. Именно поэтому можно говорить о том, что эти отношения возникают у очень специфических регулирующих субъектов. На протяжении долгого времени Интернет не воспринимался государством как предмет международно-правового научного исследования. В статье проанализированы международные акты международных межправительственных организаций и международных конференций, которые связаны напрямую с управлением Интернетом, их сотрудничество можно разделить на несколько областей, которые связаны с обыденной деятельностью оперативного характера, а также с ролью правительств и выполнением их основополагающих обязанностей на международной арене. Управление Интернетом в международном праве является многогранной моделью, в сущность которой входит партнерство стран в данной сфере. Выявлена специфика механизма контроля за управлением Интернетом, которая была исторически заложена в тот момент, когда он только начал формироваться. Если рассматривать с одной стороны, то можно сказать, что Интернет зародился в рамках ММПО, с другой стороны, он

тесно взаимосвязан со Всемирным саммитом информационного общества, на котором впоследствии были разработаны основополагающие нормы для регулирования информационно-коммуникационной сети.

Ключевые слова: Интернет, контроль, международное право, международные организации, правоотношения, регулирование, технологическое изобретение

PROBLEMS OF INTERNATIONAL LEGAL REGULATION OF INTERNET MANAGEMENT

Abstract. The article examines the technical architecture of the Internet, which determines the content of institutions and entities involved in legal relations on the Internet, and the need for legal supervision over their use, identifies the fundamental importance at the national and international level, which contributed to the development of many forms of Internet governance, for which the main principle is the participation of all parties. Since the Internet is a multi-level network of technical information, it can be said that its activities are carried out within the established limits. At the same time, it is impossible to accurately determine the object and subject of the management of legal relations related to the use of the Internet. The above-mentioned legal network control relations apply to software and hardware for connecting various parts of the data transmission network in different countries, including the root server system that directs the main data flow on the Internet, channels and equipment of the physical connection, technical standards and methods for the actual implementation of network addresses of the communication device, and much more. That is why it can be said that these relations arise from very specific regulatory entities. For a long time, the Internet was not perceived by the state as a subject of international legal scientific research. The article analyzes international acts of international intergovernmental organizations and international conferences that are directly related to Internet governance, their cooperation can be divided into several areas that are related to everyday operational activities, as well as directly related to the role of governments and the fulfillment of their fundamental responsibilities in the international arena. Internet governance in international law is a multifaceted model, the essence of which includes the partnership of countries in this area. The specifics of the mechanism of control over the management of the Internet were historically laid down at the moment when the Internet was just beginning to form. If we consider on the one hand, it can be said that the Internet originated within the framework of the IMPO, on the other hand, the Internet is closely interconnected with the World Summit of the Information Society, at which the fundamental norms for regulating the information and communication network were subsequently developed.

Keywords: Internet, Control, International law, International organizations, Legal relations, Regulation, Technological invention

В начале XXI в. благодаря быстрому развитию Интернета (глобальной трансграничной информационной сети) и свободному доступу к нему для всего населения мира пользование им стало частью повседневной жизни. Приоритетным вопросом в области информационных технологий остается вопрос о международном контроле сети Интернет, что является одним из наиболее важных примеров современной

глобализации. Предметная область соответствующих правоотношений включает в себя следующих субъектов: пользователей Интернета, поставщиков услуг доступа в Интернет (обычно операторов связи), создателей и установщиков определенной информации в Интернете (например, владельцев контента, менеджеров веб-сайтов).

В обозначенных выше правоотношениях по контролю могут участвовать различные государства в лице своих законодательных и правоохранительных органов, которые занимаются вопросами незаконного использования сети Интернет на внутригосударственном уровне.

В настоящее время техническая архитектура Интернета, которая определяет содержание институтов и субъектов, вовлеченных в правовые отношения в Интернете, и необходимость правового надзора за их использованием приобрели основополагающее значение на национальном и международном уровне. Способствовало развитию многих форм управления Интернетом, для которых основным принципом является участие всех сторон.

Поскольку Интернет – это многоуровневая сеть технической информации, можно сказать о том, что ее деятельность осуществляется в установленных пределах. При этом невозможно точно определить объект и субъект управления правоотношениями, связанными с использованием Интернета.

Вышеупомянутые правовые отношения по контролю за Сетью распространяются на программное и аппаратное обеспечение для подключения различных частей сети передачи данных в разных странах, включая систему корневых серверов, которая направляет основной поток данных в Интернете, каналы и оборудование физического соединения, технические стандарты и методы фактической реализации сетевых адресов устройства связи и многое другое. Именно поэтому можно говорить о том, что эти отношения возникают у очень специфических регулирующих субъектов.

На протяжении долгого времени Интернет не воспринимался государством как предмет международно-правового научного исследования. Это связано с тем, что в глобальном масштабе не существует институционального механизма управления Сетью. Однако это не следует учитывать, поскольку в Интернете нет правовой основы для международных правовых норм.

Обращаясь к международным механизмам, нужно помнить, что развитие новых технологий приводит к появлению чего-то нового.

Новизна и сложность заключаются в том, что действия, связанные с Интернетом, влияют на способность стран координировать свои общественные потребности в этой области или заключать международный договор, когда он считается частью международного права в контексте создания международной межправительственной организации.

Управление Сетью является основным вопросом международного правового контроля за информационными технологиями. Четкого решения этой проблемы нет, но теоретические (theoretical) методы разрешения спорных ситуаций являются различными.

Однако Интернет не следует рассматривать с точки зрения «технологического изобретения», поскольку его использование влияет на внутреннее экономическое и социальное развитие различных стран и обеспечивает коммуникационные

связи между странами, организациями и людьми на международном уровне. Этот термин в полном смысле выражает значимость описываемого явления, а также установление и соблюдение правил и процедур деятельности и развития глобальных сетей.

На данный момент известно несколько методов, которые в полной мере позволяют осуществлять контроль за деятельностью интернет-пользователей. Из этого вытекают несколько основных подходов, которые в полной мере позволяют решить возникшие в деятельности по контролю спорные моменты.

Одним из них является наиболее широкий подход, который включает в себя технические и социально- политические вопросы управления Интернетом [1].

Безусловно, необходимо отметить тот факт, что управление Интернетом на международном поле привело к возникновению вопроса о создании единого информационного общества, понятие которого было конвенционно закреплено в «Окинавской хартии Глобального информационного общества» [2].

В большинстве международных актов международных межправительственных организаций и международных конференций, которые связаны напрямую с управлением Интернетом, их сотрудничество можно разделить на несколько областей, которые связаны с обыденной деятельностью оперативного характера, а также с ролью правительств и выполнением их основополагающих обязанностей на международной арене.

Управление Интернетом в международном праве является многогранной моделью, в сущность которой входит партнерство стран в данной сфере.

Данная многогранная модель была сформирована посредством деятельности делового, а также технического характера, которая полностью охватила субъекты международно-частных правоотношений, а также субъекты публичных правоотношений на международном уровне. По словам Н. Н. Гончаровой: «Несмотря ни на что, государственно-частное партнерство является механизмом развития государства и общества и нацелено на решение трудоемких, затратных и достаточно рискованных программ национального и международного значения» [3].

Необходимо сказать о том, что правительство играет значительную роль благодаря исполнению своих обязательств на международной арене, которые прежде всего фокусируются на контроле внутригосударственной и внешней политики по регулированию информационной сети. По словам Г. Г. Шинкарецкой: «Другим местом образования норм, в которых прямо и непосредственно не участвуют государства, являются неправительственные организации» [4].

Обозначенная выше многогранная модель регулирования интернет-пространства исходит из того, что государство как субъект данных правоотношений не властно над информационно-коммуникационной сетью и ни одно государство при возникновении негативных условий не имеет права запретить индивидам из разных стран пользоваться Интернетом.

При этом техническая составляющая информационно-коммуникационной сети подпадает под юрисдикцию внутреннего законодательства различных государств. Национальное законодательство определенного государства при возникновении

каких-либо спорных моментов или угрозы национальной безопасности может наложить временные ограничения на передачу информации по данной сети.

Именно поэтому специфика механизма контроля за управлением Интернетом была исторически заложена в тот момент, когда он только начал формироваться. С одной стороны, можно сказать, что интернет зародился в рамках ММПО (далее – международная межправительственная организация), с другой – он тесно взаимосвязан с Всемирным саммитом информационного общества, на котором впоследствии были разработаны основополагающие нормы для регулирования информационно-коммуникационной сети.

Отметим, что становление Интернета приобрело приоритетное значение после принятия двух основополагающих международных источников. Таких как «Декларация принципов информационного общества» [5], а также «План действий встречи мирового уровня по информационному обществу».

Данные акты впоследствии установили нормы для управления Интернетом, который гласит, что каждая сторона, которой заинтересована в конкретном вопросе, но при этом имеет различные интересы, может взаимодействовать друг с другом.

После проведения саммита были названы основные направления, которые требовали наибольшего внимания, а именно:

1. Вопрос безопасности и национальной стабильности государств при использовании сети Интернет.

2. Вопрос об использовании сети Интернет на международном уровне.

3. Вопрос о контроле за распространением запрещенной информации в международном пространстве.

4. Вопрос о защите информации и личных данных субъектов в информационном пространстве и многие другие.

Однако после проведения встречи механизмы, которые регулируют управление Интернетом на международном уровне, так и не были созданы. Взамен их рабочая группа, которая отвечала за контроль в сфере управления Интернетом, предложила внедрить четыре основных направления по регулированию управления Сетью.

В период проведения саммита на международном уровне активно обсуждался вопрос объединения деятельности по управлению Интернетом между государствами, а также возможности государствам самим присваивать веб-адреса в Сети. Предполагалось создание особенной ММПО, которая бы объединила на международном поле деятельность по управлению Интернетом.

В идеальном представлении эта ММПО не подчинялась бы какому-то государству конкретно, а включила в себя унифицированные нормы управления Интернетом для глобального сотрудничества между государствами.

Но лидеры нескольких государств не оказали поддержки для создания новой ММПО с возможностью передачи полномочий для осуществления деятельности по управлению Интернетом. Они полагали, что передача полномочий может привести к полному уничтожению информационно-коммуникационной сети, потому что организация не сможет в полной мере реализовать идеализированные принципы глобальной сети. Также передача полномочий позволит странам-участницам активно нарушать права индивидов и тайну их частной жизни.

Следует сказать о том, что в настоящее время существуют ММПО, которые обладают возможностью регулировать управление информационной сетью. Это такие организации, как Всемирная организация интеллектуальной собственности, Международный союз электросвязи и, конечно же, Организация Объединенных Наций.

Обозначенные выше ММПО проводят активное взаимодействие с субъектами международного частного права по различным проблемам управления Интернетом. При этом уставная деятельность ММПО напрямую связана с выполнением установленных задач, которые закреплены в актах проведенного саммита.

Существует еще одна особенность в деятельности ММПО, она заключается в том, что в процессе работы межправительственных организаций были образованы различные группы и комиссии, которые участвуют в сфере управления Интернета.

Однако в вышеназванных объединениях есть свои нюансы.

Во-первых, они действуют согласно мандату, в котором определен круг вопросов.

Во-вторых, они состоят из заинтересованных субъектов.

В-третьих, они носят декларативный характер.

Обратим внимание на тот факт, что ММПО на данный момент активно развиваются и сотрудничают друг с другом в сфере управления Интернетом.

Выводы. Значимость ММПО в вопросах, касающихся контроля и регулирования сети Интернет, была закреплена после подписания документов саммита, которые носили завершающий характер.

Особое место принадлежит МСЭ, деятельность которого тесно связана с информационно-коммуникационными технологиями. Предполагается, что контроль за управлением сети Интернет в ближайшее время будет усилен во многих странах, например, в России, Европе, Бразилии, Иране, Пакистане и др. Призыв Европейского союза к наращиванию потенциала поддерживается не во всех государствах, включая эти страны, и не учитывает интересы представителей сторон, которые занимаются вопросами дистанционного управления.

Список литературы

1. Истомин Н. А. Модель участия заинтересованных сторон в управлении Интернетом на международном уровне // Право и политика. 2020. № 5. URL: https://cyberleninka.ru/article/n/model-uchastiya-zainteresovannyh-storon-v-upravlenii-internetom-na-mezhdunarodnom-urovne (дата обращения: 17.09.2022).

2. Окинавская хартия Глобального информационного общества // Дипломатический вестник. 2000. № 8. С. 51–56.

3. Гончарова Н. Н. Государственно-частное партнерство в России и регионах как форма сотрудничества государства и частных субъектов // БГЖ. 2014. № 3 (8). URL: https://cyberleninka.ru/article/n/gosudarstvenno-chastnoe-partnerstvo-v-rossii-i-regionah-kak-forma-sotrudnichestva-gosudarstva-i-chastnyh-subektov (дата обращения: 19.09.2022).

4. Шинкарецкая Г. Г. Взаимодействие законодательства различных государств в процессе цифровизации государственного управления // Образование и право. 2021. № 1. URL: https://cyberleninka.ru/article/n/vzaimodeystvie-zakonodatelstva-

razlichnyh-gosudarstv-v protsesse-tsifrovizatsii-gosudarstvennogo-upravleniya (дата обращения: 19.09.2022).

5. Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии. URL: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения: 18.09.2022).

О. А. Киселева,
кандидат юридических наук, доцент,
Омский государственный университет имени Ф. М. Достоевского

МЕЖДУНАРОДНАЯ И НАЦИОНАЛЬНАЯ ПРАВОВЫЕ СИСТЕМЫ В КОНТЕКСТЕ РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Информация, а вслед за ней и информационные технологии – чрезвычайно динамичная область человеческой деятельности. Динамика обуславливает возникновение потребности в упорядочении, в том числе посредством такого социального регулятора, как право. Правовое регулирование требуется не только и не столько на внутригосударственном уровне, сколько на международном. В первую очередь с помощью формулирования и закрепления более универсальных и единообразных норм, которые смогут быть детализированы и конкретизированы уже в национальном праве.

Ключевые слова: информационное право, информационные технологии, международное право, национальное право, международный договор, регионализация, принципы права

INTERNATIONAL AND NATIONAL LEGAL SYSTEMS IN THE CONTEXT OF INFORMATION TECHNOLOGY REGULATION

Abstract. Information, and information technology, is an extremely dynamic area of human activity. The dynamics causes the emergence of the need for streamlining, including through such a social regulator as law. Legal regulation is required not only and not so much at the domestic level, but precisely at the international level. First of all, through the formulation and consolidation of more universal and uniform norms that can be detailed and concretized already in national law.

Keywords: Digital law, Information technology, International law, National law, International treaty, Regionalization, Principles of law

Если обратиться к сегодняшней системе международно-правовых отношений, то можно констатировать такую весьма внутренне противоречивую тенденцию. С одной стороны, происходит эскалация скептицизма к данной правовой системе, как утрачивающей былую фундаментальность, а с другой – становится все более очевидна даже невооруженным глазом крайняя необходимость международного нормативно-правового регулирования, без которого современные цивилизации рискуют самоуничтожиться.

Акторы международного сообщества, которые понимают изложенное, налаживают конструктивный и продуктивный диалог и коллаборацию («коллаборация» – слово, пришедшее из французского языка, в дословном переводе это работа (с кем-то) или сотрудничество).

В тренде современного диалога России с членами Евразийского экономического союза, Шанхайской организации сотрудничества и других организаций находятся inter alia вопросы правового регулирования информационных технологий, Digital Law, IT-сфера.

В сущности, с развитием технологий и скорости передачи информации, а также объемов этой информации становится понятно, что любое государство уже не справится, если будет сохранять регулирование данных областей только в сфере внутренней компетенции.

Как подчеркивает М. Н. Марченко, «тенденции развития государственно-правовых явлений на глобальном уровне не существуют изолированно от тенденций их эволюции на региональном и национальном уровнях» [6. С. 100]. Таким образом, международная правовая система и национальные правовые системы современных государств неизбежно в ходе эволюционного (а хотелось бы именно таким его видеть) развития общества и его социальных регуляторов приходят в синергию.

Отмечается, что «международное право является «утилитарной материей, в основе которой должны лежать базовые универсальные для всего человечества ценности независимо от политического устройства, религиозных догматов, культуры и т. д.» [7. С. 184–189].

Так или иначе, но информационные технологии приходят во взаимодействие с такими базовыми, универсальными ценностями.

Формально-юридически для целей настоящего исследования допустимо использовать интерпретацию, предлагаемую в ст. 1 Федерального закона «Об информации, информационных технологиях и о защите информации»:

1. Информация – сведения (сообщения, данные) независимо от формы их представления.

2. Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Касательно предлагаемого определения термина «информация», например, профессор А. В. Морозов высказывает сомнения в его верности, выражая симпатию философскому определению информации как отраженному разнообразию [12. С. 75].

В сущности, информационные технологии представляют собой процессы, которые так или иначе протекают с информацией, технические решения, которые сопровождают информацию в пути ее следования от источника к адресату, а мы лишь дополняем это правовым контекстом. Таким образом, информация является объектом правоотношений, а развитие сети Интернет выводит эти правоотношения на уровень как минимум трансграничных отношений и как максимум – международных.

И даже если отношения, связанные с информационными технологиями, находятся в национальной правовой плоскости, мы всегда держим в уме следующее.

Часть 4 ст. 15 Конституции РФ устанавливает, что общепризнанные принципы и нормы международного права и международные договоры РФ являются составной частью ее правовой системы. Если международным договором РФ установлены иные правила, чем предусмотренные законом, то применяются правила международного договора [4].

При этом законодательство РФ об информации, информационных технологиях и о защите информации основывается на Конституции РФ, международных договорах РФ и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов (п. 1 ст. 4 ФЗ № 146-ФЗ).

Таким образом, правовое регулирование в области информационных технологий не является исключительно областью внутригосударственного правового регулирования. Обращаясь к особенностям международного нормативного регулирования, нельзя не упомянуть об общих тенденциях функционирования данной правовой системы в целом.

На сегодняшний день можно выделить следующие основные тенденции развития международного права:

1. В области международного права происходит существенная трансформация сферы источников.

Прослеживается сокращение базы нормативных актов международного права, нарастает тенденция к использованию «обычаев», которые, в силу схожести формы существования, фактически подменяются «правилами» [5. С. 1; 1; 2. С. 35–60].

На первый план выходит доктрина (концепция «избранного международного общества», доктрина «гуманитарной интервенции»). Несмотря на часто весьма взвешенные мнения ученых в области международного права, такой вспомогательный источник международного права обладает некоторыми отрицательными. В частности, доктрина подвержена «инъекциям» междисциплинарных исследований, которые (опять же в силу существенной специфики международного права не только применительно к иным наукам в целом гуманитарного профиля, но к наукам внутригосударственного права) не всегда позволяют говорить о достоверности полученных результатов ввиду недостатков эмпирической базы в области именно международного права. Доктрина создается учеными – личностями, которые, так или иначе, подвержены влиянию своих правовых культур и патриотизму, что несет риск попыток обосновать или подвергнуть критике явления международной действительности в угоду соответствующему влиянию.

Кроме того, отдельными государствами международного сообщества делаются попытки не только создать самостоятельную (сильно отличающуюся от международной правовой системы) систему, основанную на правилах, но и вывести с места вспомогательных на место основных такие источники права, как рекомендательные акты международных организаций. Особо циничные попытки такой деятельности имеют место на сегодняшний день в рамках деятельности Генеральной Ассамблеи ООН [10].

Отмечаются и весьма закономерные и перспективные попытки иных акторов международного права активизировать обращение в качестве правового обоснования

своей позиции к основополагающим принципам международного права (принцип добросовестного выполнения международных обязательств, принцип нерушимости государственных границ и вытекающее из него право на самооборону и пр.).

1. Все это вызывает фрагментацию международного права, которая проявляется в избирательности реализации международно-правовых норм.

2. Толкование норм международного права нередко даже компетентными субъектами осуществляется в угоду какого-то интереса, а не на основе принципа справедливости и верховенства права. Это закономерно увеличивает объем обращения к категориям «предвзятость» и «пристрастность», что снижает эффективности международных судебных учреждений и способность создать стабильность в области применения норм международного права.

3. Все это, в свою очередь, подрывает доверие к международному праву и незыблемым институтам международного права (международным судам, ООН, основным принципам международного права).

4. И, наконец, регионализация. При этом с определенной долей поправок можно констатировать эффективность развития региональных интеграционных наднациональных образований. Можно также констатировать интереснейшую тенденцию: «…с одной стороны, в сфере универсального международного права наблюдается сокращение базы источников международного права <…> с другой стороны, в области региональной международной интеграции, напротив, количество источников международного правового регулирования увеличивается, а процесс их реализации интенсифицируется» [3. С. 58].

5. В области утверждения обязательности и исключительности своих правил и порядков отдельными акторами международных отношений активно используется информационное давление, дезинформация (фейк), нарушение принципов свободы слова и цензуры, а фактически это все складывается в полноценные механизмы информационной войны, в которой применяется информационное оружие [14. С. 43–53]. Такая тенденция рушит само основание информационной безопасности как на общемировом уровне, так и на индивидуальном.

Анализ действующего нормативного массива международного права свидетельствует об отсутствии комплексных международных договоров в области обеспечения эффективного, правового функционирования информационных технологий.

Более того, можно применительно к международному правовому регулированию именно вопросов информационных технологий констатировать следующие особенности:

1. Любые международные общественные отношения должны быть урегулированы нормами международного права в строгой иерархической последовательности. Во главе такой иерархии стоят основные принципы международного права, которые подлежат непосредственному применению. Данное обстоятельство подтверждается и доктринальными исследованиями, в рамках которых ученые последовательно доказывают тот факт, что на киберпространство также распространяются основные принципы права [13. С. 102–107; 15. С. 458–459; 16. С. 9; 8. С. 77–81].

Следующий уровень – это основные источники международного права, к коим традиционно относятся международные договоры и обычаи.

В числе международных договоров, которые регулируют отношения, связанные с информацией, информационными технологиями и защитой информации, значатся такие, как:

а) Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г. № 108 (вступила в силу для России 01.09.2013);

б) Конвенцию Совета Европы об информации относительно иностранного законодательства 1968 г. № 62 (вступила в силу для России 13.05.1991);

в) Конвенцию Совета Европы о преступности в сфере компьютерной информации 1991 г. (Россия принимала активное участие в ее разработке, но не подписала ее);

г) Декларацию принципов построения информационного общества (Declaration of Principles WSIS-03/Geneva), принятую на Всемирной встрече на высшем уровне в Женеве в декабре 2003 г.

Также существует ряд двусторонних международных договоров в указанной сфере, например, Соглашение между Правительством Республики Беларусь и Правительством РФ о сотрудничестве в области защиты информации 1997 г.; Соглашение между Правительством Российской Федерации и Правительством Республики Индонезия о сотрудничестве в области обеспечения международной информационной безопасности (заключено в Джакарте 14.12.2021); Соглашение между Правительством Российской Федерации и Правительством Республики Никарагуа о сотрудничестве в области обеспечения международной информационной безопасности (заключено в Москве 19.07.2021) и др.

В качестве специфического источника международного права нужно назвать акты международных организаций, которые по своей сути направлены на унификацию правового регулирования в отдельных областях информационных технологий. Например, постановление № 14–7.1 Парламентской ассамблеи организации договора о коллективной безопасности «О проекте модельного закона ОДКБ «Об информационной безопасности».

Сделаем замечание, которое не должно было остаться без внимания: 15 марта 2022 г. Российская Федерация сделала официальное заявление о запуске процедуры выхода из Совета Европы, что фактически означает не только прекращение в установленном порядке юрисдикции Европейского суда по правам человека, но и ставит вопрос о том, как международные договоры, принятые в рамках данной организации, будут действовать в отношении России. Сдержанный комментарий на эту тему прозвучал уже в заявлении, согласно которому «положения основных договорно-правовых актов Совета Европы включены в российское законодательство» [9]. Но Венская конвенция о праве международных договоров 1969 г. не предусматривает такого основания для прекращения действия в отношении субъекта международного права положений международного договора. Для этого требуется денонсация или выход из соответствующих документов, которые пока не совершены Россией.

Вместе с тем классические вспомогательные источники международного права, такие как судебный прецедент (судебная практика) [17] и доктрина, также функционируют в рамках интересующей нас области общественных отношений в сфере

International Digital Law. Но в силу отсутствия как раз универсальных международных договоров (на что непосредственно оказывают влияние общие тенденции международного права, о которых шла речь выше) вспомогательным источникам крайне сложно формироваться, потому что системность права никто не отменял. Сначала нормы должны создаваться, и только потом они могут быть реализованы.

2. Исследование вопросов цифровых технологий и Digital Law становится все более востребованным, ученые активно формируют базу цифровых прав, к которым относят право на забвение, право на защиту персональных данных, право на доступ к Интернету и др. [11]. При этом часто такие права выводятся из тех личных прав человека, которые закреплены в Билле о правах, носят характер международных стандартов прав человека и только с появлением информационных технологий получили новую интерпретацию.

3. Развитие информационных технологий – это не просто двусторонний процесс: с одной стороны, это обеспечение каждого свободно получать и распространять информацию, с другой – это обязанность государства и мирового сообщества защищать тот объем информации, который носит персонифицированный характер, защищать общество от дезинформации, обеспечиваться свободу выражения мысли и др.

Все же тут возникает еще одна сторона, где требуется особая правовая защита соответствующей информационной технологии, которая является произведением интеллектуального труда, что накладывает отпечаток на технологические процессы по обеспечению этой функции. Встречно здесь возникает злоупотребление со стороны создателей программ и сервисов в части своих авторских прав (это является самостоятельной темой для дискуссии).

4. В связи с отсутствием должного правового регулирования в области информационных технологий, обеспечивающих доступность различного рода услуг коммерческих предприятий и государственных органов, происходит существенное искажение права человека на сохранность его персональных данных inter alia на свободу выбора предоставления таких данных и выдачи разрешения на их обработку и использование. Такое право фактически трансформировалось в обязанность, при этом совершенно без каких-либо на то объективных нормативных обоснований.

Изложенные характеристики международной правовой системы и системы правового регулирования цифровых технологий свидетельствуют о необходимости скрупулезной, вдумчивой и междисциплинарной работы по выработке стандартов международно-правового регулирования. Очевидно, что пока такие стандарты могут быть приняты только в рамках международных организаций, где не заблокирована деятельность России. Но и о планомерной и регулярной постановке вопроса в стенах Организации Объединенных Наций речь также идет, Россия обладает потенциальной способностью к продвижению проектов нормативных актов, хоть он и нивелирован некоторыми механизмами из информационной сферы.

Начатая гармонизация и унификация международного и национального права в данном случае должна сыграть весомую роль в формировании устойчивой правовой среды для информационных технологий.

То есть мы можем сделать вывод о том, что информация может влиять на реализацию, по сути, всех основных прав человека, а также может становиться самостоятельным объектом правового регулирования.

Особенностью коллаборации международного и внутригосударственного правового регулирования в данной области можно назвать то обстоятельство, что в силу специфики нормообразования в международном праве такие динамичные общественные отношения вынужденно становятся более урегулированными на уровне внутренней правовой системы с ожиданием последующего переноса или выхода с предложением о переносе методов и средств регулирования в плоскость международного права.

Кроме того, приходится констатировать, что стандарты правового регулирования информационных технологий в большей степени создаются сейчас на государственном или региональном уровне, но не на уровне универсального международного права. А учитывая единство правового пространства, различие в стандартах еще долго будет тормозить эффективность.

Список литературы

1. Бен Скотт. Порядок, основанный на правилах: что скрывает название // Россия в Глобальной политике. 24.08.2021. URL: https://globalaffairs.ru/articles/poryadok-na-pravilah-chto-eto/? (дата обращения: 01.04.2022).

2. Вылегжанин А. Н., Нефедов Б. И., Воронин Е. Р., Магомедова О. С., Зотова П. К. Понятие «порядок, основанный на правилах» и международное право // Московский журнал международного права. 2021. № 2. С. 35–60.

3. Киселева О. А. Теоретико-прикладные аспекты взаимодействия международной и национальной правовых систем // Правоприменение. 2022. № 6 (1). С. 58. URL: https://doi.org/10.52468/2542–1514.2022.6(1)

4. Конституция Российской Федерации принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // СПС «Консультант Плюс».

5. Лавров. С. В. О праве, правах и правилах // Коммерсантъ. № 109/П от 28.06.2021.

6. Марченко М. Н. Глобализация и основные тенденции развития национальных и наднациональных государственно-правовых систем в XXI веке. Москва: Проспект, 2019.

7. Марочкин С. Ю., Безбородов Ю. С. Упущенная возможность как грядущая неизбежность // Россия в глобальной политике. 2018. Т. XVI, № 1. С. 184–189.

8. Мороз Н. О. Международно-правовые основы обеспечения международной информационной безопасности // Труд. Профсоюзы. Общество. 2016. № 1 (51). С. 77–81.

9. Официальный сайт Постоянного представительства Российской Федерации в Совете Европы. URL: https://coe.mid.ru/-/zaavlenie-mid-rossii-o-zapuske-procedury-vyhoda-iz-soveta-evropy?inheritRedirect=true (дата обращения: 10.09.2022).

10. Резолюция ГА ООН «Агрессия против Украины». Док. ООН. Distr.: Limited A/ES-11/L.1 1 March 2022. URL: https://reliefweb.int/sites/reliefweb.int/files/resources/RU_105.pdf (дата обращения: 07.03.2022).

11. Рожкова М. А. Цифровые права в контексте международного права // Закон.ру. 2021. 11 мая. URL: https://zakon.ru/blog/2021/5/11/cifrovye_prava_v_kontekste_mezhdunarodnogo_prava (дата обращения: 10.09.2022).

12. Цифровая трансформация: вызовы праву и векторы научных исследований: монография / под общ. ред. А. Н. Савенкова; отв. ред. Т. А. Полякова, А. В. Минбалеев. Москва: РГ-Пресс, 2021. 344 с.

13. Beard J. M. Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law // Vanderbilt Journal of Transn. Law. 2014. Vol. 47, № 1. Pp. 67–144.

14. Denning D. Reflections on Cyberweapons Controls // Computer Security Journal. 2000. Vol. XVI, № 4. Pp. 43–53.

15. Kondoch B. Jus ad Bellum and Cyber Warfare in Northeast Asia // Journal of East Asia and Int. Law. 2013. Vol. 6. Pp. 473–474.

16. Lawrence T., Goodman S. E., Soo Hoo K. J. Greenberg. Information warfare and international law. Washington: Nat. Defense Univ. Press, 1998. 53 p.

17. New technologies. September 2022. URL: https://www.echr.coe.int/documents/fs_new_technologies_eng.pdf (дата обращения: 10.09.2022).

В. Б. Криштаносов,
кандидат экономических наук, докторант,
Белорусский государственный технологический университет

РЕГУЛИРОВАНИЕ ЦИФРОВОЙ ЭКОНОМИКИ НА МЕЖДУНАРОДНОМ УРОВНЕ

Аннотация. В статье исследуются проблемы формирования регуляторной экосистемы международных организаций для становления и развития цифровой экономики. Цифровизация, являясь по своему характеру эндогенным, технологическим фактором экономического развития, становится важным его институтом в современных условиях. С учетом нарастания новых рисков и угроз, обусловленных повсеместным внедрением цифровых технологий, их трансграничным характером, усиливается необходимость соответствующего международного регулирования. Автором выделены особенности регулирования цифровой экономики со стороны международных организаций, определены недостатки сформированной регуляторной экосистемы и возможные направления ее оптимизации.

Ключевые слова: цифровая экономика, регуляторная экосистема, международное регулирование, кибербезопасность, международные организации, институты ООН, FATF

REGULATION OF THE DIGITAL ECONOMY AT THE INTERNATIONAL LEVEL

Abstract. The article examines the problems of the formation of the regulatory ecosystem of international organizations for the formation and development of the digital economy. Digitalization, being by its nature an endogenous, technological factor in economic development, is becoming an important institution in modern conditions. Taking into account the growth of new risks and threats caused by the widespread introduction

of digital technologies, their cross-border nature, the need for appropriate international regulation is increasing. The author highlights the features of regulation of the digital economy by international organizations, identifies the shortcomings of the formed regulatory ecosystem and possible directions for its optimization.

Keywords: Digital economy, Regulatory ecosystem, International regulation, Cybersecurity, International organizations, UN institutes, FATF

Четвертая промышленная революция меняет бизнес-модели, создавая не только общие возможности, но и риски в области экономической безопасности, на которые государства вынуждены реагировать. Международное сотрудничество позволяет решать проблемы цифровизации экономики, обеспечения кибербезопасности более эффективно, используя механизмы обмена информацией, экспертизой, объединяя ресурсы и осуществляя совместные действия для достижения целей и задач экономического развития. Особенностью цифровой экономики является ее глобальный характер, который не позволяет нивелировать риски и угрозы в рамках отдельных юрисдикций без наднационального взаимодействия.

Важнейшее значение приобретают координация и сотрудничество между регулирующими и правоохранительными органами для противодействия угрозам цифровизации в условиях, когда в отдельности ни одна юрисдикция не может самостоятельно гарантировать защищенную киберсреду.

В настоящее время элементами программ и стратегий цифровизации, как правило, выступают институциональные блоки: механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; регулирования финансового рынка; защиты киберпространства (рис. 1).

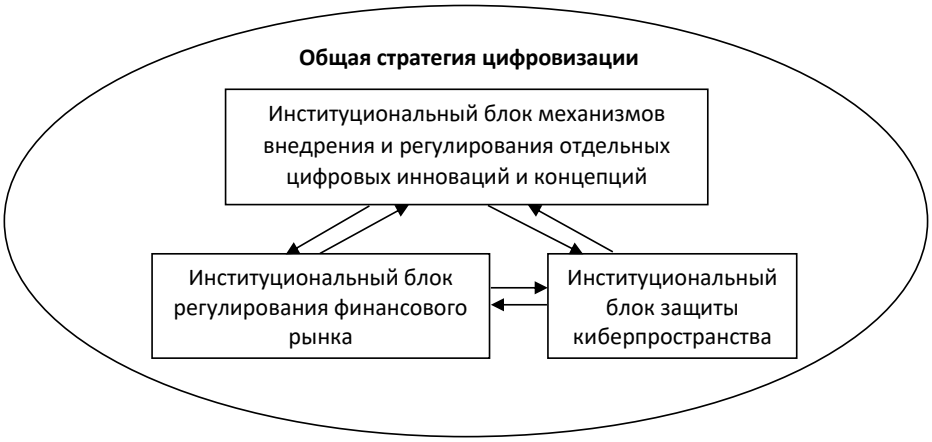

Рис. 1. Элементы институциональной регуляторной экосистемы цифровой экономики. *Источник*: разработано автором.

Моделирование основных составляющих стратегий и институциональных блоков формирования современной международной экосистемы цифровой экономики на первом и втором уровнях позволяет сформировать следующую институциональную матрицу (табл. 1).

Таблица 1

Регуляторная институциональная матрица международной экосистемы (уровень международных организаций) цифровой экономики

Уровень	Институц. блок	Название организации (документа), год создания (принятия)	Основной объект регулирования в сфере цифровизации
Уровень универсальных международных организаций	СЦ	ООН: Цели устойчивого развития (ЦУР), 2015	Расширение внедрения цифровых технологий в экономику
	ИБЦИ	ООН: Международный союз электросвязи (ITU), 1947	Обеспечение всеобщего доступа к информации и связи
		ООН: Всемирный банк, 1944	Адаптация цифровых возможностей для развития экономики и повышения благосостояния населения
	ИБФР	ООН: МВФ, 1944	Подготовка рекомендаций регуляторам в сфере FinTech в разрезе обеспечения стабильности функционирования национальных и международной финансовых систем
		ООН: Конференция по торговле и развитию ООН (ЮНКТАД), 1964	Подготовка рекомендаций в сфере FinTech в разрезе обеспечения стабильности финансовой системе
	ИБЗК	ООН: Международная стратегия по уменьшению опасности стихийных бедствий (UN ISDR), 1999	Методология оценки устойчивости критической инфраструктуры к киберугрозам

Сокращения: СЦ – стратегия цифровизации; ИБЦИ – институциональный блок механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; ИБФР – институциональный блок регулирования финансового рынка; ИБЗК – институциональный блок защиты киберпространства

Источник: разработано автором.

Анализ табл. 1 показывает, что международный уровень экосистемы регулирования цифровой экосистемы охватывает организации системы ООН, ориентированные на развитие различных областей цифровой экономики. В 2015 г. были утверждены Цели устойчивого развития ООН (ЦУР) [1], которые встраиваются, по мнению ряда исследователей [2. С. 2–3], в концепцию цифровизации экономики и внедрения современных цифровых технологий: AI, Smart City, Blockchain и прочих – в различные сферы производства. Международная стратегия ООН по уменьшению опасности стихийных бедствий (UNISDR) выводит основные критерии оценки устойчивости критической

инфраструктуры к внешним шокам [3. С. 632–641][1]. Проблематикой адаптации экономических систем к цифровым вызовам занимаются МВФ и Всемирный банк. МВФ в 2021 г. выступил с предложениями о необходимости глобального регулирования криптоактивами и формирования глобальной нормативной базы, включающей такие элементы, как лицензирование поставщиков услуг, связанных с криптоактивами, которые выполняют критически важные функции; адаптация регуляторных требований к основным вариантам использования криптоактивов и стейблкоинов. Официальные органы должны предъявлять четкие требования к регулируемым финансовым организациям в отношении их открытых позиций и операций с криптоактивами [4].

Координация по выработке политики и стратегии стабилизации финансовых систем в условиях цифровых рисков также осуществляется на уровне G20. В 2010 г. G20 признала финансовую доступность в качестве одного из основных столпов глобальной повестки дня в области развития, одобрила План действий по финансовой доступности и создала Глобальное партнерство по финансовой доступности (GPFI)[2]. В 2016 г. GPFI выпустило отчет «Органы, устанавливающие мировые стандарты, и финансовая доступность: развивающийся ландшафт», в котором отразило последствия развития FinTech относительно защиты потребителей, развития конкуренции и совместимости (проведение транзакций в разных финансовых сетях); защиты персональных данных; краудфандинга; управления риском. Кроме того, опубликованы «Принципы высокого уровня G20 для цифровой финансовой интеграции», призванные способствовать принятию этих принципов для более широкого охвата планирования финансовой интеграции, в частности цифровой финансовой интеграции (табл. 2).

Организацией по разработке политики и регулированию финансовой доступности и FinTech является также Альянс за финансовую доступность (AFI), который согласовал подходы в нормативной отчетности, в частности в области мобильных платежей для центральных банков и банковских надзорных органов.

В 2020 г. семью государствами (Канадой, Данией, Италией, Японией, Сингапуром, ОАЭ и Великобританией) в рамках Всемирного экономического форума (WEF) подписано соглашение Agile Nations [5], направленное на расширение международного сотрудничества в сфере развития, в том числе цифровых инноваций в условиях четвертой технологической революции. Ключевые направления взаимодействия включают обмен знаниями и лучшей практикой во избежание ненужных расхождений в правилах, которые препятствуют трансграничным инновациям и совместным действиям по устранению общих рисков.

---

[1] Устойчивость критической инфраструктуры – это «…способность системы, сообщества или общества, подверженного опасности, противостоять, поглощать, приспосабливаться к последствиям опасности и своевременно и эффективно устранять их, в том числе путем сохранения и восстановления его основных структур и функций».

[2] В организации участвуют такие многосторонние организации, как Всемирный банк и Консультативная группа по оказанию помощи бедным (CGAP), Международный валютный фонд (МВФ) и ООН.

Таблица 2

Регуляторная институциональная матрица международной экосистемы (уровень специализированных международных институтов) цифровой экономики (разработано автором)

Уровень	Институц. блок	Название организации (документа), год создания (принятия)	Основной объект регулирования в сфере цифровизации
Уровень специализированных международных институтов	СЦ	–	–
	ИБЦИ	G20: Глобальный альянс Smart City, 2019	Внедрение концепции Smart City, разработка принципов ответственного и безопасного использования технологий
		Всемирный экономический форум (WEF): соглашение Agile Nations, 2020	Международное сотрудничество в условиях четвертой технологической революции, обмен знаниями и лучшими практиками в сфере цифровизации
	ИБФР	Банк международных расчетов (BIS): Базельский комитет по банковскому надзору, 1974	Разработка единых стандартов и методик регулирования банковской деятельности, включая FinTech
		Международная организация комиссий по ценным бумагам (IOSCO), 1983	Агрегирование лучших практик управления рынками ценных бумаг, включая FinTech
		Группа разработки финансовых мер борьбы с отмыванием денег (FATF), 1989	Разработка стандартов и способствование эффективному применению правовых, нормативных и оперативных мер по борьбе с отмыванием денег, финансированием терроризма, распространением оружия массового уничтожения в условиях расширения использования цифровых активов
		Банк международных расчетов (BIS): Комитет по платежам и рыночной инфраструктуре (CPMI), 1990	Разработка единых стандартов в отношении безопасности и эффективности платежных, клиринговых, расчетных и связанных с ними механизмов
		Альянс за финансовую доступность (AFI), 2008	Расширение внедрения FinTech для развития финансовой доступности, поддержка МСП
		G20: Совет по финансовой стабильности (FSB), 2009	Координация национальных финансовых органов и международных органов, устанавливающих стандарты с учетом развития FinTech
		G20: Глобальное партнерство по финансовой доступности (GPFI), 2010	Развитие финансовой доступности, FinTech в условиях обеспечения стабильности финансовых систем
		Глобальная сеть финансовых инноваций (GFIN), 2019	Масштабирование новых технологий FinTech в различных юрисдикциях
		Банк международных расчетов (BIS): Центр инноваций, 2019	Выявление критических тенденций в развитии технологий, влияющих на центральные банковские системы, и разработка соответствующих рекомендаций для центральных банков

Уровень	Институц. блок	Название организации (документа), год создания (принятия)	Основной объект регулирования в сфере цифровизации
Уровень специализированных международных институтов	ИБЗК	Международная электротехническая комиссия (IEC), 1906	Разработка международных стандартов в области электрических, электронных и смежных технологий (включая IoT)
		Международная организация по стандартизации (ISO), 1947	Разработка международных стандартов в сфере кибербезопасности
		Институт инженеров электротехники и электроники (IEEE), 1963	Разработка стандартов по радиоэлектронике, электротехнике и аппаратному обеспечению вычислительных систем и сетей (включая IoT)
		Международная ассоциация аудита и контроля информационных систем (ISACA), 1967	Сертификация специалистов в области кибербезопасности
		WEF: **«Партнерство для киберустойчивости»**, 2011	Разработка принципов, направленных на повышение системной устойчивости к киберрискам
	Сокращения: СЦ – стратегия цифровизации; ИБЦИ – институциональный блок механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; ИБФР – институциональный блок регулирования финансового рынка; ИБЗК – институциональный блок защиты киберпространства		

Регулирующие органы в разных регионах мира находят новые способы сотрудничества в управлении цифровизацией. Многие органы финансового регулирования заключили двусторонние соглашения о сотрудничестве в области регулирования («мосты взаимодействия») для облегчения совместной работы над инновациями [6. С. 40–43][1].

В 2019 г. создан Глобальный альянс умных городов G20 по управлению технологиями, который объединяет муниципальные, региональные и национальные правительства, партнеров из частного сектора вокруг общего набора принципов ответственного и этичного использования технологий умных городов. Альянс устанавливает и продвигает международные нормы, чтобы помочь ускорить внедрение передовых практик, снизить потенциальные риски и способствовать большей от-

[1] Например, валютное управление Сингапура с 2016 г. заключило 33 соглашения о сотрудничестве, охватывающие такие виды деятельности, как обмен прогнозами, практикой и поддержкой.

крытости и общественному доверию. Функции секретариата Альянса выполняет Всемирный экономический форум [7].

Уровень специализированных международных институтов представлен в первую очередь Группой разработки финансовых мер борьбы с отмыванием денег (FATF). В рамках разработки рекомендаций по выявлению и купированию рисков для национальной безопасности стран-членов данная организация осуществляет анализ современных тенденций, в том числе в области цифровизации экономики в целом и финансовых систем в частности. На основе обмена опытом стран-участниц по выявлению и купированию рисков, связанных с внедрением технологий блокчейн, использованием криптовалют для осуществления противозаконных действий, направленных в первую очередь на отмывание денег и финансирование терроризма (ПОД-ФТ). Таким образом, данный институт является ключевым в международном регулирующем пространстве в области разработки стандартов ПОД-ФТ.

FATF разработала серию «Рекомендаций», которые признаны международными стандартами по борьбе с отмыванием денег, финансированием терроризма и распространением оружия массового уничтожения. Это обеспечивает основу для скоординированных международных ответных действий, направленных на противодействие этим угрозам целостности мировой финансовой системы. В 2015 г. FATF выпустила глобальное руководство как часть поэтапного подхода к устранению рисков отмывания денег и финансирования терроризма, связанных с продуктами и услугами для оплаты виртуальных активов. В 2018 г. FATF опубликовала отчет, в котором изложены обязательства FATF по борьбе с незаконным финансированием с использованием виртуальных активов[1]. В 2019 г. FATF приняла Пояснительную записку к Рекомендациям, которая дополнительно разъясняет и расширяет поправки FATF к стандартам, касающимся виртуальных активов, и описывает, как страны и финансовые организации должны соблюдать соответствующие Рекомендации по предотвращению неправомерного использования виртуальных активов для отмывания денег, финансирования терроризма и распространения оружия массового поражения. Предложен рискориентированный подход к виртуальным активам, а также рекомендации по применению спектра превентивных мер ПОД-ФТ, включая надлежащую проверку клиентов, ведение документации, отчетность о подозрительных транзакциях и проверку транзакций на соответствие целевым финансовым санкциям. Фокусом мониторинга FATF также являются элементы цифровой инфраструктуры, включая криптобиржи [8. С. 3]. В 2021 г. опубликован доклад с рекомендациями регуляторам по мониторингу цифровых активов и введению соответствующих стандартов в отношении виртуальных активов и их поставщиков.

[1] В Рекомендациях, касающихся новых технологий, отмечается, что для управления и снижения рисков, связанных с виртуальными активами, странам следует обеспечить, чтобы поставщики услуг виртуальных активов регулировались в целях ПОД-ФТ, были лицензированы или зарегистрированы и подпадали под действие эффективных систем мониторинга и обеспечения соблюдения соответствующих мер, предусмотренных в Рекомендации FATF.

Надзор за деятельностью банков, разработка методологий оценки платежеспособности, установление стандартов банковского регулирования на глобальном уровне осуществляются через Базельский комитет по банковскому надзору Банка международных расчетов. Комитет по платежам и рыночной инфраструктуре (CPMI) Банка международных расчетов (BIS) совместно с Международной организацией комиссий по ценным бумагам (IOSCO) представил в 2021 г. Принципы инфраструктуры финансового рынка (PFMI) в отношении международного стандарта для платежей, клиринговых и расчетных систем, а также Руководство по соответствию механизмов стейблкоинов международным стандартам. Данные принципы применяются ко всем системно значимым платежным системам, центральным депозитариям ценных бумаг, системам расчетов по ценным бумагам, центральным контрагентам и торговым репозиториям. В дополнение к этим стандартам CPMI и IOSCO опубликовали ряд связанных документов и дальнейшее руководство по внедрению стандартов.

IOSCO взаимодействует с G20 и Советом по финансовой стабильности (FSB) в рамках глобальной программы реформ регулирования. FSB, объединяющий центральные банки и финансовых регуляторов из G20 совместно с МВФ, Всемирным банком, Банком международных расчетов, подготовил в 2020 г. проект рекомендаций в отношении влияния стейблкоинов на эффективность трансграничных розничных платежей [9]. В рамках своей координирующей роли FSB должен разработать основу, включающую стандарты для регулирования криптоактивов, целью которой должно стать обеспечение комплексного и согласованного подхода к управлению рисками для финансовой стабильности и поведению на рынке, который может последовательно применяться в различных юрисдикциях, и при этом сведение к минимуму возможностей для регулятивного арбитража или переноса деятельности в юрисдикции с менее строгими требованиями. Кроме того, Базельский комитет BIS дорабатывает документ с требованиями к банковской системе в отношении резервного капитала банков, которые используют криптовалюты.

Проблематика регулирования криптоактивов находится в повестке дня Большой семерки (G7) на уровне министров финансов, управляющих центральными банками, с участием Европейской комиссии, руководителей МВФ, Всемирного банка и Совета по финансовой стабильности. На саммите G20 в 2021 г. была принята декларация [10], в которой страны-участницы поддержали предложение ОЭСР по введению минимального глобального налога для транснациональных корпораций на уровне 15 %. Кроме того, отмечена значимость политики, направленной на создание раскрывающей потенциал, инклюзивной, открытой, поддерживающей честную конкуренцию цифровой экономики, которая способствует применению новых технологий, позволяет бизнесу и предпринимателям процветать, защищает и дает права потребителям. Отмечена приверженность ведущих промышленных государств международному сотрудничеству, направленному на цифровую трансформацию производства, процессов, услуг и бизнес-моделей, в том числе с помощью основанных на консенсусе международных стандартов и совершенствования защиты потребителей, развития цифровых навыков и грамотности. Выражена необходимость решения возросших проблем безопасности в цифровой среде, в том

числе от программ-вымогателей и других форм киберпреступности, а также готовность укрепления двустороннего и многостороннего сотрудничества для защиты национальных ИКТ, устранения общих уязвимостей и угроз и борьбы с киберпреступностью. По результатам встречи G20 руководители государств призвали CPMI, Центр инноваций BIS, МВФ и Всемирный банк продолжить углубление анализа потенциальной роли цифровых валют центральных банков (CBDC) в расширении трансграничных платежей и их более широких последствий для международной валютной системы. МВФ разработана операционная стратегия по дальнейшему выполнению мандата с учетом роста государственных и частных цифровых денег.

В 2019 г. 29 регулирующих органов создали Глобальную сеть финансовых инноваций (GFIN). Среди прочего сеть тестирует среду, которая позволит одновременно испытывать и масштабировать новые технологии в нескольких юрисдикциях[1].

Важным направлением международного регулирования цифровизации являются разработка и внедрение стандартов. Международная электротехническая комиссия (IEC) на международном уровне разрабатывает стандартизированные решения и практики для обеспечения методологии систематической оценки безопасности компонентов цифровых систем, чтобы гарантировать их надежную и безопасную работу. Рабочая группа Сектора стандартизации электросвязи Международного союза электросвязи (ITU) разрабатывает стандарты «умного города», каждый из которых ориентирован на различные аспекты его инфраструктуры, такие как архитектура, совместное использование данных и безопасность. Аналогичным образом рабочая группа Института инженеров электротехники и электроники (IEEE) создала группу интеллектуальных городов. Группа технологических и финансовых компаний объявила в 2017 г. о работе над стандартом для защиты приложений интернета вещей (IoT) с помощью блокчейна. На уровне платежной отрасли в 2009 г. установлены стандарты безопасности индустрии платежных карт (PCI DSS), рекомендованные организациям, которые хранят, обрабатывают или передают финансовые данные карт. В 2019 г. Международная организация по стандартизации (ISO) выпустила руководящие принципы, призванные помочь предприятиям соблюдать правила конфиденциальности и защиты данных в различных юрисдикциях.

Таким образом, в настоящее время с учетом трансграничного характера рисков и угроз как на международном, так и наднациональном уровнях происходит поступательное формирование новой системы регулирования. На международном уровне данная система включает традиционные институты системы ООН, адаптирующие

[1] GFIN – это сеть из 50 организаций, активно настроенных на поддержание финансовых инноваций в интересах потребителей. GFIN старается обеспечить более эффективный способ для инновационных фирм с целью взаимодействия с регуляторами, помогая им лавировать между странами, поскольку они имеют склонность взвешивать новые идеи. Сюда относится пилотный проект для фирм, желающих протестировать инновационные продукты, услуги или бизнес-модели на территории более чем одной юрисдикции. Она также направлена на создание новой базы для сотрудничества между регуляторами финансовых услуг по темам, связанным с инновациями, делясь различным опытом и подходами.

традиционные мандаты, механизмы и инструменты регулирования к современным вызовам цифровизации.

На уровне специализированных международных организаций, происходит интенсивная эволюция как традиционных институтов, включая IOSCO, FATF, BIS, IEC, ISO, IEEE, так и формирование новых инициатив и механизмов регулирования, в том числе созданных по решению G20, WEF и др. По причине высокой динамики внедрения новых цифровых механизмов и бизнес-моделей единое регулирование по сферам деятельности к настоящему времени отсутствует. Вместе с тем следует отметить объединение ресурсов и компетенций международных институтов для выработки совместных решений (рекомендаций) в отношении рисков, связанных с цифровыми инновациями.

Отсутствие четкого разграничения компетенций в сфере регулирования цифровой повестки создает ситуацию одновременного вмешательства различных международных институтов в регуляторные практики, в особенности в сфере цифровых финансовых технологий, что снижает ценность данных рекомендаций. В то же время некоторые сферы регулирования (например, стандартизация, IoT) являются избыточно сегментированными, и отсутствие общего регулирования не позволяет выработать общие регламенты их использования. С учетом сложности и комплексности стоящих перед наднациональными институтами задач адаптации к современным рискам и угрозам цифровой экономики растет необходимость разработки актуальных системных подходов к институционализации общих механизмов обмена опытом противодействия киберугрозам и соответствующей экспертизой на государственном и государственно-частном уровнях, а также международными техническими нормативными актами и стандартами безопасности цифровых решений, включая интернет вещей (IoT), облачные вычисления, искусственный интеллект и машинное обучение (AI/ML), большие данные (Big Data), блокчейн, FinTech и пр.

Список литературы

1. Цели в области устойчивого развития / ООН. URL: https://www.un.org/sustainabledevelopment/ru/sustainable-development-goals/ (дата обращения: 22.02.2022).

2. Dwivedi Y. et al. Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. Opinion paper // International Journal of Information Management. 2021. Vol. 57 (7). 47 p. DOI: 10.1016/j.ijinfomgt.2019.08.002

3. Pursiainen C. Critical infrastructure resilience: A Nordic model in the making? // International Journal of Disaster Risk Reduction. 2018. Vol. 27. Pp. 632–641. DOI: 10.1016/j.ijdrr.2017.08.006

4. Tobias A., Dong H., Aditya N. Global Crypto Regulation Should be Comprehensive, Consistent, and Coordinated. 2021. URL: https://blogs.imf.org/2021/12/09/global-crypto-regulation-should-be-comprehensive-consistent-and-coordinated/?utm_medium=email&utm_source=govdelivery (дата обращения: 13.12.2021).

5. May A. Public Engagement: Nations Sign First Agreement to Unlock Potential of Emerging Tech // World Economic Forum. 2020. URL: https://www.weforum.org/press/2020/12/nations-sign-first-agreement-to-unlock-potential-of-emerging-tech (дата обращения: 13.12.2020).

6. Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators // World Economic Forum. 2020. 56 p. URL: https://www.weforum.org/pages/agile-regulation-for-the-fourth-industrial-revolution-a-toolkit-for-regulators (дата обращения: 11.03.2021).

7. G20 Global Smart Cities Alliance on Technology Governance. URL: https://globalsmartcitiesalliance.org/?page_id=107 (дата обращения: 16.10.2020).

8. Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing: FATF Report. 2020. 24 p. URL: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf (дата обращения: 19.09.2020).

9. Jones H. Global watchdogs agree rules for stablecoins like Facebook's Libra. 2020. URL: https://www.reuters.com/article/us-g20-regulator-cryptoassets/global-watchdogs-agree-rules-for-stablecoins-like-facebooks-libra-idUSKBN 26X2OQ (дата обращения: 11.10.2020).

10. G20 Rome Leaders' Declaration. 2021. URL: https://www.consilium.europa.eu/media/52732/final-final-g20-rome-declaration.pdf (дата обращения: 11.11.2021).

Д. В. Лобач,
кандидат юридических наук,
доцент кафедры теории и истории государства и права,
Дальневосточный юридический институт (филиал)
Университета прокуратуры Российской Федерации

РАЗВИТИЕ И ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАКТИКЕ СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

Аннотация. В статье исследуются различные процессы, возникающие в практике современных международных отношений в связи с активным использованием информационно-коммуникационных технологий. Отмечается, что информационно-коммуникационные технологии в современных условиях становятся неотъемлемой частью нового состояния геополитического противостояния, более известного как «гибридные войны». На основании анализа современного состояния международного права в области информационной безопасности обосновываются причины снижения его регулятивного действия.

Ключевые слова: информационно-коммуникационные технологии, информационная безопасность, цифровой суверенитет, информационное право, информационные угрозы

DEVELOPMENT AND APPLICATION OF INFORMATION TECHNOLOGIES IN THE PRACTICE OF MODERN INTERNATIONAL RELATIONS

Abstract. The article examines various processes that arise in the practice of modern international relations in connection with the active use of information and communication technologies. It is noted that information and communication technologies in modern conditions are becoming an integral part of the new state of geopolitical confrontation,

better known as «hybrid wars». Based on the analysis of the current state of international law in the field of information security, the reasons for the decrease in its regulatory effect are substantiated.

Keywords: Information and communication technologies, Information security, Digital sovereignty, Information law, Information threats

В условиях интенсивного развития сквозных (дизруптивных) информационно-коммуникационных технологий (далее – ИКТ) и их широкой интеграции в различные сферы жизни общества происходит качественное изменение социальных отношений, что зачастую приводит к неоднозначным последствиям. С одной стороны, наблюдается изменение социального уклада жизни общества, приводящего к смене традиционных устоев и появлению так называемого информационного общества [8. С. 95]. Феномен информационного общества является закономерным следствием происходящей в настоящее время четвертой промышленной революции. В самом общем виде концепт «информационное общество» олицетворяет собой такую социальную организацию общества, при которой трудовой фактор (занятое население) ориентирован на производство, хранение, переработку и реализацию информации, а социальные структуры функционируют и развиваются в режиме эффективного информационного взаимодействия, имеют доступ к мировым информационным ресурсам и способны удовлетворять свои потребности в информационных продуктах и услугах. Без преувеличения можно признать, что экспоненциальное развитие и применение информационно-коммуникационных технологий в условиях становления информационного общества приводит к более эффективному управлению, снижению рисков наступления неблагоприятных последствий, развитию человеческого потенциала, росту уровня жизни, комфортности проживания, а также обеспечению общей безопасности. В этом аспекте справедливо отмечается, что в современных условиях создается цифровое общество, сопровождаемое глубокими и качественными преобразованиями, которые захватывают все отрасли экономики (промышленность, сельское хозяйство, торговлю, сферу услуг) и разные сферы жизни человека (личную, семейную, общественную), при этом цифровая эпоха перестроила все механизмы взаимодействия общества, так как новые технологии изменили формат социального взаимодействия, что обусловливает четвертую промышленную революцию в истории человечества.

С другой стороны, быстрое развитие и широкое распространение ИКТ также обусловливает новые и нарождающиеся угрозы в отношении жизни, здоровья, субъективных прав и свобод, чести и достоинства человека, собственности, общественной безопасности и правопорядка, публичных интересов общества и государства. При этом такие угрозы возникают как на национальном уровне отдельных государств, так и на международном уровне, т. е. в практике международных отношений.

Анализ результатов современных научных исследований, средств массовой информации, ведомственных аналитических отчетов и отчетов международных организаций позволяет выявить следующие тренды использования ИКТ в практике международных отношений.

Прежде всего обращает на себя внимание широкое использование ИКТ в целях создания платформ для политического диалога. Сегодня мы видим, что социальные сети удовлетворяют не только потребности простых обывателей в получении различного рода информационных услуг, но и выступают площадкой для политического диалога со стороны общественных и политических деятелей. Интересной особенностью такого общения является то, что высказанные взгляды и предложенные идеи, как правило, не отражают официальную позицию власти по тому или иному вопросу. Подобная практика, с одной стороны, упрощает восприятие политического контента (информации о политических событиях и процессах), так как подается в сжатом виде и без какого-либо оформления, что делает ее более адаптивной для обыденного правосознания. С другой стороны, это может создавать когнитивный диссонанс, поскольку одни и те же политические события и процессы по-разному будут отражаться в медиапространстве.

По мере развития ИКТ наблюдается активная изощренная деятельность международных информационных агентств по конъюнктурному освещению тех или иных событий, происходящих в мировой политике. Такое освещение событий очень часто сопровождается искажением и умолчанием о конкретных фактах, а равно наблюдается откровенная фальсификация определенных фактов в целях оправдания своей позиции и создания образа врага или агрессора. В практике международных отношений с настораживающей периодичностью проявляются случаи фальсификации каких-либо событий и фактов в целях осложнения международных отношений или дестабилизации обстановки внутри другого государства. При этом полная или частичная фальсификация событий означает искажение партикулярных ситуаций (единичные убийства, отравления, скандалы), вызывающих закономерный общественный резонанс. Фальсификация фактов связана с искажением исторической памяти народа в целях создания отрицательного образа публично-правового образования (народ, нация, государство, часть государства). Зачастую искажение исторических фактов происходит в целях дискредитации национального политического режима. В других случаях искажение фактов позволяет запустить процесс принятия в отношении отдельных государств недружественных актов, что предопределяет агрессивную политику и осложнение международных отношений. В этом ключе нельзя не отметить позицию Жана Бодрийяра, в соответствии с которой современные политические процессы сопровождаются имитацией, гиперсимуляцией и агрессивной симуляцией [1. С. 23–29]. И действительно, сегодня мы с вами видим, что международные политические отношения зачастую развиваются без учета объективных процессов и реальных событий, а также сопровождаются искаженными нарративами. Так, в недавнем прошлом хорошо известны случаи, когда широкое медийное освещение непроверенной, а зачастую прямо искаженной информации о преступлениях режимов в Ираке, Ливии и Сирии способствовало инспирированию политической реакции и инициированию военных операций в этих странах. Сегодня мы становимся свидетелями того, как в информационном пространстве создается агрессивный образ России, КНДР, КНР, Белоруссии и ряда других государств.

Информационное пространство в целом и медийная сфера в частности становятся некой площадкой для вбрасывания деструктивного контента, с тем чтобы

оказать прямое или опосредованное информационно-психологическое воздействие и сформировать в обществе нужное (или ненужное) отношение к правящему режиму власти. В свою очередь, подготовка населения той или иной страны к действиям в нужном направлении также может свидетельствовать о попытках лигитимизации возможного применения вооруженной силы против неугодного режима, что, в сущности, и отражает механизм практики так называемых цветных революций. К сожалению, ситуация во многом осложняется еще и тем обстоятельством, что если раньше фальсификацию новостей в пропагандистских целях осуществляли государственные структуры, обладающие необходимыми для этого знаниями и дорогостоящим оборудованием, то в современных условиях такая возможность доступна практически каждому. В научной литературе справедливо отмечается, что повышение доли поддельного контента, имеющего высокий уровень реалистичности, угрожает не столько отдельным лицам или брендам, сколько самому обществу, основанному на информации, а также добрососедским отношениям между разными странами. Возможности для распространения фальсифицированной информации в условиях электронной культуры разнообразны: новостные ленты в электронных СМИ, социальные сети, личные блоги, персональные страницы, выкладываемые в Интернет видеофайлы (например, в «YouTube»), СМС-рассылка по мобильной связи и многое другое. Формы фальсификации информации также существенно различаются.

Развитие информационных технологий позволяет перевести избирательный процесс и государственное управление в цифровую форму, что демонстрирует реализацию идеи цифрового государства или цифрового правительства. Вместе с тем подобная трансформация создает условия для вмешательства во внутренние дела другого государства посредством совершения кибератак, что приводит к осложнению международных отношений. Безотносительно к тому, насколько эти атаки реальны и возможно ли вообще в техническом плане оказать какое-либо влияние на избирательный процесс, хорошо известны случаи обвинения Российской Федерации в том, что якобы русские хакеры совершили ряд атак на электронную систему голосования в США, приведших к искажению результатов выборов.

Хакерские атаки, как элемент кибероружия, и специальные технологии по сбору информации вообще становятся неотъемлемой частью современного информационного общества и сопутствующей практикой международных отношений. Так, еще в 2006 г. австралийский интернет-журналист и телеведущий основал международную некоммерческую организацию WikiLeaks, занимающуюся сбором из анонимных источников секретной информации и последующим ее опубликованием. Другим, не менее известным примером, иллюстрирующим сбор и распространение секретной информации, является деятельность американского технического специалиста и спецагента Эдварда Сноудена, который в 2013 г. опубликовал секретную информацию американских спецслужб, доказывающую тотальную слежку этих служб в информационном пространстве за гражданами многих государств по всему миру. Как известно, оба события оказали существенное влияние на межгосударственное сотрудничество и динамику международных отношений.

Отдельно следует сказать об изменении содержательной части международных отношений в том смысле, что активное внедрение ИКТ в политический процесс,

выражаемый не только в освещении политических событий, но и в генерировании новых событий, оказывающих влияние на политическую обстановку в самих государствах и на международной арене, отодвигает государства на второй план. Это обстоятельство свидетельствует не только о трансграничном характере ИКТ, но также и о подрыве роли государств как традиционного актора международных отношений. Подобная ситуация становится возможной, поскольку размывается традиционное понимание государственного суверенитета.

В современной практике международных отношений ИКТ также используются в целях обеспечения национальных интересов через применение так называемой мягкой силы, под которой понимается форма внешнеполитической стратегии, предполагающая способность добиваться желаемых результатов на основе добровольного участия, симпатии и привлекательности, в отличие от жесткой силы, которая подразумевает принуждение. О политическом значении мягкой силы также заявляется и на национальном уровне. Так, в п. 9 Концепции внешней политики Российской Федерации (утверждена Президентом Российской Федерации В. В. Путиным 30 ноября 2016 г.) закреплено, что «неотъемлемой составляющей современной международной политики становится использование для решения внешнеполитических задач инструментов “мягкой силы”, прежде всего возможностей гражданского общества, информационно-коммуникационных, гуманитарных и других методов и технологий, в дополнение к традиционным дипломатическим методам» [7].

Следует также отметить, что ИКТ в современных условиях становятся неотъемлемой частью нового состояния геополитического противостояния, более известного как гибридная война. Несмотря на широкое междисциплинарное изучение данного явления и разные подходы в понимании содержательной стороны гибридной войны, большинство исследователей и политических деятелей признают, что ИКТ становятся важным инструментом, который используется в целях подрыва социального мира и нарушения государственного управления. В специальной литературе справедливо отмечается, что современное геополитическое противостояние, сочетающее в себе как непосредственно традиционные военные угрозы, так и нетипичные формы агрессивной политики, направленные против суверенитета и политической независимости других государств, также охватывает различные формы манипуляции в информационном пространстве [2. С. 30–31; 6]. Действительно, проведенные за последние 20 лет интервенции и цветные революции в разных странах достоверно доказывают нам, что информационное пространство становится новым театром противостояния. Что касается информационной составляющей в контексте понимания феномена гибридной войны, то она охватывает такие проявления информационной войны, как пропаганда, фейковые новости, стратегические утечки, психологические формы манипулирования.

Представленные выше проблемы, связанные с деструктивными и агрессивными формами использования ИКТ в практике международных отношений, обусловливают постановку вопроса о международно-правовом регулировании отношений в области информационной безопасности. Нельзя не отметить, что в настоящее время международная информационная безопасность является объектом правового

регулирования со стороны ряда универсальных документов. Так, в период с 1998 по 2021 г. Генеральной Ассамблеей ООН было принято более 30 резолюций, направленных на обеспечение информационной безопасности [4]. На региональном уровне в разное время были приняты и действуют международные договоры в области обеспечения информационной безопасности: Концепция информационной безопасности государств – участников Содружества Независимых Государств в военной сфере 1999 г.; Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности 2009 г.; Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г.; Конвенция Совета Европы «О преступности в сфере компьютерной информации» 2001 г.; Конвенция Лиги арабских государств «О борьбе с преступлениями в области информационных технологий» 2010 г. [5].

Однако современное состояние международного права в сфере обеспечения информационной безопасности не отражает в полной мере те вызовы и тренды, которые возникают в условиях интенсивного развития и применения ИКТ на современном этапе.

Во-первых, универсальные документы, принятые по линии Генеральной Ассамблеи ООН, являются актами «мягкого права», т. е. их нормы носят политико-правовой характер и не порождают юридических последствий. Взятые во всем своем многообразии резолюции ГА ООН могут стать основой для перспективной кодификации норм в сфере информационной безопасности.

Во-вторых, отсутствие единой международной конвенции в сфере информационной безопасности лишь отчасти компенсируется действием вышеуказанных региональных конвенций, так как, несмотря на общий вектор правового регулирования, отсутствует нормативная унификация в части определения общего понятийно-категориального аппарата, информационных угроз, которые посягают на отношения в информационной среде, а также закрепления целей и приоритетных направлений противодействия этим угрозам.

В-третьих, попытки выработки эффективного механизма правового регулирования отношений в сфере информационной безопасности в практике межгосударственного сотрудничества обременены объективными сложностями, связанными с границами государственного суверенитета. В эпоху интенсивного развития информационных отношений происходит размывание границ государственного суверенитета, так как информационное пространство и происходящие там процессы приобретают наднациональный характер и не могут регулироваться государственными органами власти [3, 10]. Эта проблема находит свое отражение в академической среде, где все чаще оперируют таким понятием, как «цифровой суверенитет», под которым в самом общем представлении понимают способность государства проводить свою политику в информационной сфере [9. P. 35–51].

В-четвертых, отсутствие консолидированного международного договора, регулирующего отношения в сфере информационной безопасности, во многом объясняется политикой двойных стандартов и стремлением отдельных государств доминировать в сфере информационных технологий.

В заключение необходимо отметить, что ИКТ, взятые во всем своем многообразии, будучи необходимой частью информационного общества, цифровой экономики и электронного правительства, также активно используются в практике международных отношений. В целом использование ИКТ в практике современных международных отношений можно выразить в двух направлениях: 1) ИКТ создают необходимые платформы для межгосударственного взаимодействия и политического процесса; 2) ИКТ используются как некий инструмент проведения агрессивной политики. Что касается обеспечения информационной безопасности в практике международных отношений посредством создания необходимого для этих целей механизма международно-правового регулирования, то эта задача может быть решена только при условии широкого взаимодействия и сотрудничества, а также соблюдения национальных интересов отдельных государств и всего международного сообщества. Представляется, что в обстановке критического недоверия между государствами, блокового характера международных отношений, проводимой политики двойных стандартов и безапелляционного стремления отдельных стран англосаксонского мира к мировому доминированию, основанному на искаженном представлении о своей исключительности, проблема эффективного обеспечения информационной безопасности в практике международных отношений будет оставаться нерешенной еще долгое время.

Список литературы

1. Бодрийяр Ж. Симулякры и симуляции / пер. с фр. А. Качалова. Москва: ПОСТУМ, 2015.

2. Калдор М. Новые и старые войны: организованное насилие в глобальную эпоху / пер. с англ. А. Апполонова, М. Дондуковского; ред. перевода А. Смирнов, В. Софронов. Москва: Изд-во Института Гайдара, 2015.

3. Формирование национального цифрового суверенитета в условиях дифференциации пространственного развития / Л. С. Леонтьева, М. В. Кудина, А. С. Воронов, С. С. Сергеев // Государственное управление. Электронный вестник. 2021. № 84. URL: https://cyberleninka.ru/article/n/formirovanie-natsionalnogo-tsifrovogo-suvereniteta-v-usloviyah-differentsiatsii-prostr

4. Информационно-коммуникационные технологии / Официальный сайт ООН. URL: https://www.un.org/ru/development/ict/res.shtml

5. Международная информационная безопасность: теория и практика: в 3 т. Т. 2: Сборник документов (на русском языке) / под общ. ред. А. В. Крутских. Москва: Аспект Пресс, 2019.

6. Тиханычев О. В. Гибридные войны: новое слово в военном искусстве или хорошо забытое старое? // Вопросы безопасности. 2020. № 1.

7. Указ Президента РФ от 30.11.2016 № 640 «Об утверждении Концепции внешней политики Российской Федерации» // СПС «КонсультантПлюс».

8. Шваб К. Четвертая промышленная революция. Москва: Эксмо, 2016.

9. Duarte M. E. Network Sovereignty: Building the Internet across Indian Country. Seattle, WA: University of Washington Press, 2017.

10. Hui Li, Xin Yang. Co-governed Sovereignty Network: Legal Basis and Its Prototype & Applications with MIN Architecture. Springer, 2021.

Т. Н. Михалева,
кандидат юридических наук, доцент,
Белорусский государственный университет

ЦИФРОВАЯ ПОВЕСТКА ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА: ОТ ИДЕИ К ПРАВУ

Аннотация. Цифровая трансформация повседневной жизни, бизнес-среды, государственного управления требует не только внедрения инновационных правовых и институциональных инструментов, но и создания единого цифрового пространства в рамках Евразийского экономического союза (далее – Союза, ЕАЭС). Сочетание согласованной и единой политики видится необходимым для успешной реализации многофакторной, полисубъектной информационно-цифровой стратегии Союза. На повестке ЕАЭС – 2025 стоит развитие цифровой инфраструктуры внутри общего рынка и в институтах ЕАЭС, кибербезопасность и защищенность процессов. Нарастание социотехнического взаимодействия неизбежно приведет и к расширению евразийской цифровой повестки: качественно новые типы общественных отношений (цифровая реальность) потребуют инновационного регулирования, диверсификации механизмов управления, аксиологической «переустановки» и в целом перехода от информационного взаимодействия в рамках Союза, цифровизации как инструмента – к цифровой модели ЕАЭС, созданию Единого евразийского цифрового пространства.

Ключевые слова: гармонизация; Евразийский экономический союз; Евразийская экономическая комиссия; единая политика; единое цифровое пространство; информационное взаимодействие; информационно-коммуникационные технологии; право ЕАЭС; региональная интеграция; согласованная политика; стратегия цифровой трансформации; унификация; цифровая интеграция; цифровая повестка ЕАЭС

DIGITAL AGENDA OF THE EURASIAN ECONOMIC UNION: FROM IDEA TO LAW

Abstract. The digital transformation of everyday life, the business environment, and public administration requires not only the introduction of innovative legal and institutional instruments, but also the creation of a common digital space within the EAEU. The combination of a coherent and unified policy is seen as necessary for the successful implementation of a multifactor, multi-subject infomark and digital strategy of the Union. The EAEU-2025 agenda includes the development of digital infrastructure within the common market and the EAEU institutions, cybersecurity and process security. The increase in socio-technical interaction will inevitably lead to the expansion of the Eurasian digital agenda: qualitatively new types of social relations (digital reality) will require innovative regulation, diversification of governance mechanisms, axiological "resetting" and, in general, the transition from information interaction within the Union, digitalization as a tool – to the EAEU digital model, the creation of the Common Eurasian Digital Space.

Keywords: Harmonization, Eurasian Economic Union, Eurasian Economic Commission, Common policy, Common digital space, Information interaction, Information and communication technologies, EAEU law, Regional integration, Coordinated policy, Digital transformation strategy, Unification, Digital integration, EAEU digital agenda

Введение. О включении цифровой повестки в современные интеграционные процессы. Региональная интеграция стала активным трендом межгосударственного взаимодействия в конце XX – начале XXI в. В частности, об этом свидетельствует и экспоненциальный рост нотификаций региональных торговых соглашений в ВТО (RTA Database, WTO, 2021). Не все из них являются институализированными организациями с продвинутым уровнем интеграции, однако в каждом регионе есть интеграционные проекты различной степени интенсивности и успешности [10].

Понятие «интеграция» происходит от латинского integratio – обеспечение целостности, восстановление целостности, от корневого integer – целостный. В Большом российском энциклопедическом словаре интеграция определяется как состояние связанности отдельных дифференцированных частей и функций системы, организма в целое, а также как процесс, ведущий к такому состоянию [1]. Межгосударственная интеграция определяется как процесс, обеспечиваемый международно-правовыми средствами и направленный на постепенное образование межгосударственного, экономически, а возможно, и политически единого, целостного (integro) пространства, зиждущегося на общем рынке обращения товаров, услуг, капиталов и рабочей силы [2]. Свобода передвижения данных факторов производства стала визитной карточкой экономико-правовой характеристики межгосударственной интеграции и отражена в таком объеме практически во всех учредительных актах региональных интеграционных объединений (например, п. 1 ст. 1 Договора о Евразийском экономическом союзе, п. 2 ст. 26 Договора о функционировании Европейского союза).

Построение единого рынка в современном мире было бы не только неполным без включения цифровой повестки в правовую и организационную материю интеграционных объединений, но и малоэффективным. Проникновение цифровых технологий и главенство информационно-коммуникативного элемента в любых современных отношениях отразилось и на формировании повестки интеграционных объединений. Так, в 2014 г. в ЕС стартовала Стратегия цифрового рынка – спустя 7 лет после перехода Европы к этапу экономического и валютного союза на основании Лиссабонского договора.

В ЕАЭС цифровая повестка была запущена в 2016 г., менее чем через два года после подписания Договора о Евразийском экономическом союзе. В декабре 2020 г. премьер-министр Российской Федерации на Первом Евразийском конгрессе предложил, что к четырем свободам рынка должна добавиться еще одна – свобода движения информации. В настоящее время предложен комплекс мероприятий по формированию Единого цифрового пространства. При этом изначально в учредительных актах Союза заложена готовность к цифровой трансформации экономики

и общественных отношений, базирующаяся на ряде общих и специальных норм договора, несмотря на то, что буквально в тексте употребляются категории, связанные прежде всего с информационным обеспечением интеграционных процессов и информационным взаимодействием.

Основная часть. О понятиях «информатизация», «цифровизация», «цифровая трансформация». В научной литературе справедливо указывают на отличие понятий «информатизация» и «цифровизация», анализируя экономические, правовые смыслы, онтологию информационных и цифровых контекстов [17. С. 39] Некоторые исследователи употребляют их как синонимичные или схожие [23. С. 17]. В зарубежной литературе обращают внимание на различие понятий «цифровизация» и «оцифровка» [27. P. 45]. В отличие от первого, означающего прогрессивное использование цифровых технологий и цифровой информации, которые приводят к изменениям в функционировании вещей и социальном контексте, второе – лишь перевод данных из аналогового в цифровой формат.

Ряд ученых отмечают включение в цифровые процессы вопросов информатизации, своеобразный переход от информатизации к цифровизации [13. С. 110]. А. Паулин, напротив, оценивает цифровизацию как процесс, предшествующий информатизации общества [26. P. 259]. Цифровизация, по его мнению, отражает современное развитие общества, технологий и как таковую концепцию экономики 4.0. В то же время информатизации и как ее продолжению – информатизированному управлению данный автор пророчит широкое применение во всех отраслях и сферах в скором будущем, но не сейчас.

Согласно СТБ 2583-2020 «Цифровая трансформация. Термины и определения», вступившему в силу 1 марта 2021 г., цифровизация – это новый этап автоматизации и информатизации экономической деятельности и государственного управления, процесс перехода на цифровые технологии, в основе которого лежит не только использование для решения задач производства или управления информационно-коммуникационных технологий, но также накопление и анализ с их помощью больших данных в целях прогнозирования ситуации, оптимизации процессов и затрат, привлечения новых контрагентов и т. д. Цифровая трансформация – проявление качественных, революционных изменений, заключающихся не только в отдельных цифровых преобразованиях, но в принципиальном изменении структуры экономики, в переносе центров создания добавленной стоимости в сферу выстраивания цифровых ресурсов и сквозных цифровых процессов.

Цифровизация затрагивает все сферы общественной жизни, поэтому стало возможным вести речь о «цифровом императиве развития». [15, 16] Действительно, цифровизация и цифровая трансформация стали неотъемлемой частью государственных программ, концепций, экономических стратегий. Эти процессы заняли прочное место в развитии общества, в том числе ввиду особого значения для перехода к шестому технологическому укладу.

Доктринальное осмысление того, как производительность и конкурентность факторов производства, экономических акторов в любой форме зависят от возможностей генерировать, обрабатывать, безопасно и оперативно использовать информацию, основанную на знаниях, началось еще в конце XX в. [9].

Сегодня цифровые технологии, перевод бизнес-процессов в онлайн, Интернет вещей, электронное правительство и даже искусственный интеллект – эти и многие иные достижения цифровизации становятся привычными. Встают и новые задачи производного порядка – доступ к цифровым общественным благам, распределение ответственности за управление пользования Интернетом, безопасность процессов (Резолюция Генеральной Ассамблеи ООН A/C.3/74/L.11 «Противодействие использованию информационно-коммуникационных технологий в преступных целях»). Однако главное состоит в том, что конструирование новых отношений приводит к важнейшей трансформации – возникновению кибер-пространственности. Цифровой компонент переходит из фактора, опосредующего реальность, оказывающего на нее влияние, в ее определяющий. Цифровая реальность как качественно новый тип общественных отношений только раскрывается перед нами [22. С. 102]. Соответственно, зарождается новое право – «право второго модерна», регулирующее различного рода отношения в контексте цифровой реальности, Big Data, роботизированных систем, искусственного интеллекта [6].

Об информационном взаимодействии в ЕАЭС. Договор о ЕАЭС создавался как закрепление уже достигнутых интеграционных результатов (в этот период можно констатировать функционирование таможенного союза, например) и как новый этап развития, переход к экономическому союзу в классическом его понимании. Тем не менее нельзя не отметить знаковое наличие уже в первоначальном тексте Договора о ЕАЭС положений об информационном обеспечении интеграционных процессов (ст. 23). В данной статье и в Протоколе об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза, являющегося приложением № 3 к Договору о ЕАЭС (далее – Протокол об ИКТ), были предусмотрены принципы информационного взаимодействия «при реализации общих процессов в рамках Союза», а политика в области информатизации и информационных технологий была выведена в ранг согласованной политики. Эти положения требуют некоторого пояснения.

Согласно п. 2 Протокола об ИКТ, «общие процессы» – «это операции и процедуры, регламентированные (установленные) международными договорами и актами, составляющими право Союза, и законодательством государств-членов, которые начинаются на территории одного из государств-членов, а заканчиваются (изменяются) на территории другого государства-члена». Перечень общих процессов в рамках Союза определен Решением Коллегии Комиссии от 14 апреля 2015 г. № 29 и включает 76 позиций по 18 направлениям информационного взаимодействия, в том числе в сфере взаимодействия таможенных органов, по вопросам охраны и защиты прав на объекты интеллектуальной собственности, в сфере обращения лекарственных средств и медицинских изделий, технического регулирования; применения ветеринарно-санитарных мер; транспортного (автомобильного) контроля; производства и обращения сельскохозяйственной продукции; конкурентной политики и государственных (муниципальных) закупок; обеспечение электронного документооборота между государствами – членами Евразийского экономического союза и Евразийской экономической комиссией и проч.

По ряду указанных вопросов, например, по вопросам тарифного и нетарифного регулирования, технического регулирования, санитарных и фитосанитарных мер и ряда иных в праве Союза установлено требование проведения единой политики отраслевого регулирования. Единая политика согласно ст. 2 Договора о ЕАЭС предполагает применение государствами-членами унифицированного правового регулирования, в том числе на основании решений органов Союза. В консультативном заключении от 4 апреля 2017 г. Судом ЕАЭС была сформулирована правовая позиция о том, что для отнесения определенной сферы к единой политике необходимо соответствие следующим условиям: 1) наличие унифицированного правового регулирования; 2) передача государствами-членами компетенции в данной сфере органам Союза в рамках их наднациональных полномочий.

Все вопросы информационного взаимодействия, которые в современном мире зачастую являются решающими для достижения эффективного и оперативного результата, де-юре отнесены к согласованной политике в соответствии с п. 3 ст. 23 Договора о ЕАЭС. Согласованная же политика предполагает гармонизацию правового регулирования, то есть сближение законодательства государств-членов, направленное на установление сходного (сопоставимого) регулирования (ст. 2 Договора о ЕАЭС).

Это несоответствие унифицированного стандарта материально-правового регулирования и информационного потенциала сдерживает развитие интеграции. Очевидно, что в сферах, отнесенных к единой политике, необходимо установление единой политики и в отношении их информационного обеспечения. Без единого информационного поля, основанном на унификации и стандартизации информационного процесса, обмен информацией будет недостаточно эффективным [12. С. 130].

Тем более, что понимание этого на уровне реализации общих процессов есть. Так, информационное взаимодействие при реализации средствами интегрированной информационной системы внешней и взаимной торговли общего процесса «Формирование, ведение и использование единого реестра фармацевтических инспекторов Евразийского экономического союза» урегулировано в рамках единой политики путем принятия соответствующего Решения Коллегии Евразийской экономической комиссии от 25 октября 2016 г. № 127, утверждающего правила, регламент информационного взаимодействия, описание форматов и структур электронных документов и сведений, используемых для реализации средствами интегрированной информационной системы внешней и взаимной торговли указанного общего процесса, порядок присоединения к данному общему процессу.

Процесс подготовки аналогичных актов и в иных сферах общих процессов свидетельствует об общей тенденции именно унификации, а не гармонизации информационного взаимодействия. На совещании по согласованию технологических документов, регламентирующих информационное взаимодействие при обеспечении транспортного (автомобильного) контроля на внешней границе ЕАЭС (правил, регламента и т. п.) стороны указывали на необходимость четкого закрепления на уровне актов прямого действия требований к ряду информационных процедур, например, внесения уведомлений в базу данных.

Таким образом, на практике те сферы информационного взаимодействия, которые требуют унифицированного подхода с точки зрения предмета регулирования, также регулируются единообразно, на основании норм прямого действия актов Комиссии. Де-юре, тем не менее, в Договоре о ЕЭАС все еще закреплена общая норма о согласованной политике в сфере информационного взаимодействия. Полагаем, назрела необходимость внесения поправок в Договор о ЕАЭС путем уточнения положений п.3 ст. 23 с тем, чтобы в отношении тех вопросов, по которым проводится единая политика, было указано и на унифицированное регулирование информационного взаимодействия.

От информатизации к цифровизации. В отличие от «информатизации» термин «цифровизация» не употребляется в Договоре о ЕАЭС и приложениях к нему. Тем не менее исходя из текста Договора мы можем сделать вывод об использовании уже в учредительном акте Союза, в том числе на уровне терминов и дефиниций, элементов построения цифрового общества. Так, в Протоколе об ИКТ урегулированы многие вопросы электронного документооборота, использования электронной цифровой подписи. Эти аспекты являются неотъемлемой частью построения киберсоциальных учетных систем на любом уровне. [4. С. 24–25]. Внедрение киберсоциальных систем представляет новый этап развития Индустрии 4.0 и имеет решающее значение для инноваций и конкурентных преимуществ [8].

В Договоре, кроме того, заложено еще одно важное для построения цифрового общества в рамках интеграционного объединения понятие «трансграничное пространство доверия». Формирование пространства доверия предназначено для свободного обмена данными и электронными документами, защищенности информационно-телекоммуникационных сетей, информационной безопасности. Функционирование трансграничного пространства доверия обеспечивается в соответствии с Концепцией использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов, утвержденной Решением Совета Евразийской экономической комиссии от 18.09.2014 № 73, Стратегией развития трансграничного пространства доверия, утвержденной Решением Коллегии Евразийской экономической комиссии от 27.09.2016 № 105, Положением об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденным Решением Коллегии Евразийской экономической комиссии от 28.09.2015 №125, Решением Совета Евразийской экономической комиссии от 5.12.2018 № 96 «О требованиях к созданию, развитию и функционированию трансграничного пространства доверия».

Анализ этого сегмента документов показывает высокий уровень правовой проработки архитектуры построения и функционирования трансграничного пространства доверия на наднациональном уровне. Важной частью успеха реализации данного направления информационного взаимодействия будет надлежащая имплементация требований, содержащихся в данных актах, в национальных сегментах интегрированной информационной системы, особенно в части защиты данных и безопасности.

Нельзя не отметить широкий и комплексный характер ряда определений в Протоколе об ИКТ. Например, «защита информации» регламентирована как «принятие и реализация комплекса правовых, организационных и технических мер по определению, достижению и поддержанию конфиденциальности, целостности и доступности информации и средств ее обработки с целью исключения или минимизации неприемлемых рисков для субъектов информационного взаимодействия». В этой дефиниции заложены одновременно и принципы оборота информации, и основы информационной безопасности, и единство категорий социального (информация) и физического (средств ее обработки) контекста. Представляется достаточно удачным формулирование в Договоре и Протоколе об ИКТ инфраструктурных компонентов в рамках построения трансграничного пространства доверия, которые потенциально могли и были в скором времени дополнены.

Нам видится такое восприятие текста Договора и приложений к нему как заложившего базовые константы дальнейшего развития Союза в условиях цифровизации наиболее соответствующем интересам сторон и интеграционного объединения, поскольку, как отмечалось выше, продвижение свобод рынка невозможно без создания единых информационно-коммуникационных сетей, а высокая динамика цифровых отношений выдвигает на первый план сочетание гибкости технического регулирования и стабильности фундаментальных основ. Так, в условиях развития концепции цифрового суверенитета принцип суверенного равенства государств, заложенный в Договоре о ЕЭАС как базовый принцип интеграции, приобретает новые направления реализации, но не меняет свою сущность. В то же время формирование, например, общих протоколов безопасности использования ИКТ, защиты персональных данных может и должно происходить оперативно и унифицированно, для чего требуется активная правотворческая позиция Комиссии. Мысль о необходимости «опережающего эффекта» права в эпоху цифровизации и роли в этом принципов права [24] в интеграционном образовании имеет также свое приложение. Договор приобретает особое значение не только как учредительный акт организации, институализирующий основы интеграции (институализирующая функция Договора), и как регулятор единого рынка (регулятивная функция Договора), но и как акт, определяющий вектор взаимодействия в интеграционном пространстве (прогностическая функция Договора). В этом случае возрастает роль Суда ЕАЭС и динамического толкования права Союза.

Цифровой потенциал ЕАЭС раскрывается не только через интенсификацию и трансформацию внутреннего рынка, но и возможность «создания глобального логистического коридора между Европой и Азией», в отношении которого эффективна будет сопоставимость с форматами ЮНСИТРАЛ и др. Цифровая глобализация как новый этап глобализации [3] также может и должен базироваться на региональных союзах.

Таким образом, Договор обеспечил нормативно-правовую и организационно-правовую основу для создания единого цифрового пространства, одновременно автономного и безопасного внутри Союза и когерентного с внешними системами. Это позволило в течение короткого срока выйти на общую цифровую повестку Союза.

О цифровой повестке ЕАЭС и едином цифровом пространстве. Приступая к выполнению цифровой повестки ЕАЭС, важно оценить перспективы и риски, обобщить их в научной концепции цифровизации интеграционного права. Ученые справедливо указывают на цифровую трансформацию интеграции, синергетический эффект в достижении интеграционных целей [21].

Адаптация существующего права к новым цифровым отношениям возможна, но без создания новых норм не обойтись [20. С. 15]. Этот тезис в полной мере относится и к интеграционному праву.

Не вполне можно согласиться с выводом о том, что «специфической чертой модели ЕАЭС является выделение направлений и приоритетных инициатив как основы проработки проектов государственно-частного партнерства», аспектом которой «является политико-правовая модель интеграции», закрепленная в соответствующих инструментах цифровизации [25].

Программный метод используется в различных видах и в иных интеграционных объединениях. Например, в ЕС также применяется стратегическое планирование, разработка общих приоритетов, метод открытой координации (Strategy: the European Commission`s Priorities). Что действительно могло бы стать инновационным с точки зрения правового прогнозирования и программно-стратегического планирования, особенно в динамичную цифровую эру, это системная кратко-, средне- и долгосрочная постановка (и корректировка при необходимости) целей и задач.

В настоящий момент действует ряд основных актов стратегического характера по цифровой повестке: план мероприятий по реализации Основных направлений развития механизма «единого окна» в системе регулирования внешнеэкономической деятельности, утвержденный Решением Высшего Евразийского экономического совета от 8 мая 2015 г. № 19, Основные направления реализации цифровой повестки Евразийского экономического союза до 2025 г., утвержденные Решением Высшего Евразийского экономического совета от 11 октября 2017 г. № 12, Концепция трансграничного информационного взаимодействия, утвержденная Решением Евразийского межправительственного совета от 9 августа 2019 г. № 7.

В Решении Высшего Евразийского экономического совета от 11 декабря 2020 г. «О стратегических направлениях развития экономической интеграции до 2025 года» направление 5 посвящено формированию цифрового пространства Союза, цифровых инфраструктур и экосистем и включает в себя девять основных сегментов цифровой трансформации: прослеживаемость товаров в ЕАЭС, трансграничное пространство доверия и электронный документооборот, интегрированная информационная система Союза, цифровые экосистемы (в том числе оборот данных, защита персональных данных), цифровая трансформация в сфере интеллектуальной собственности, электронная торговля, внешняя цифровая повестка, повышение технического обеспечения цифровизации (беспрепятственный интернет-трафик) и совершенствование механизмов проработки инициатив и реализации проектов.

Анализируя эти трэки цифровой трансформации, следует отметить, с одной стороны, их комплексность (от технического оснащения к единым информационным системам), но с другой – их, в основном, торгово-экономический характер. Активно же развивающийся Союз необходимо воспринимать и как новое инфор-

мационное пространство. Возникновение нового информационного пространства требует системных антиэнтропийных механизмов, прежде всего аксеологических, ценностных установок. На ялтинской конференции, проводимой журналом «Международная жизнь» ежегодно, в 2017 г. прозвучала идея об актуализации общей исторической памяти и важности управления информационными потоками для формирования позитивного имиджа в массовом сознании, привлекательности государств-участников ЕАЭС в том числе вовне, на международной арене.

С точки зрения цифровизации вопрос расширения информационного присутствия, позитивного «брендирования» евразийского интеграционного проекта видится в создании собственного домена первого (верхнего) уровня. Все официальные сайты в настоящее время размещены на домене «.org» – eurasiancommission.org, courteurasian.org. Этот домен первого уровня используется большинством международных организаций и в целом представляется удобным и достаточно безопасным. Однако с точки зрения определения евразийского взаимодействия как выходящего за пределы классического международного сотрудничества к созданию наднационального интеграционного проекта, со своей парадигмой развития, стратегией внутреннего и внешнего позиционирования, т. е. создания евразийского «бренда», переход евразийских акторов (официальных союзных органов, дополнительных интеграционных неправительственных организаций, юридических и физических лиц-резидентов ЕАЭС и т. п.) может стать сильным аргументом прогресса евразийской интеграции, реализации Единого цифрового пространства.

Вопрос о регистрации в ICANN домена верхнего уровня .EA, по аналогии с доменом Европейского союза .EU обсуждался в 2014 г., однако идея не реализована. Безусловно, при регистрации такого домена верхнего уровня речь будет идти и о том, чтобы администратором такого домена был сам Союз, что потребует наделения его органов специальной компетенцией в данной сфере, то есть достижения соответствующих договоренностей между государствами-членами. Соответственно, ЕАЭС сможет устанавливать правила для пользователей, в том числе такого рода, чтобы сайты и ресурсы располагались на серверах в пределах территории Союза и др.

Не стоит забывать, что с точки зрения международного экономического права именно интеграционные объединения могут (в этом их цель, собственно) избегать условий наибольшего благоприятствования для третьих стран по тем позициям, где предоставляют в своих рамках государствам-членам более льготные условия взаимной торговли. Более того, они могут вводить ограничения во внешней торговле, исходя из интересов, угроз и рисков для интеграционного объединения. По мнению Т. Саркисяна, заместителя председателя правления ЕАБР, если поначалу ЕС ограничивался поддержкой своих собственных компаний и экосистем, то в последний год встал на путь выстраивания очевидной системы ограничений перед цифровыми корпорациями: Европейская стратегия в области данных и проект акта о цифровых рынках 2020 г. являются примерами такой системы [19]. Аналогичным образом есть все основания и в евразийском регионе сочетать развитие свободы движения информации и цифровых ресурсов со стратегией защиты информационного и цифрового Союза извне. Среди успешных проектов 2021 и 2022 гг. – работа без границ,

цифровизация госзакупок. Не менее важны и ифровое техническое регулирование, Евразийская сеть кооперации. В цифровой повестке ЕАЭС цифровая трансформация позиционируется как драйвер интеграции, в связи с чем при дальнейшем раскрытии п. 5.4 Стратегии развития ЕАЭС в реализационных актах Комиссии, международных договорах в рамках Союза следует обратить пристальное внимание на кросс-отраслевые решения и построение цифровых экосистем. Этот тренд в целом характерен для цифровой эпохи, в отношении же интеграции он особенно важен, так как способен мультиплицировать эффект перелива (spill-over effect).

Цифровизация различных отраслей экономики в масштабах интеграционного проекта должна сопровождаться поддержанием транспарентности и доступности интеграционных ресурсов, созданием единых информационно-телекоммуникационных сетей и возможностью ими пользоваться гражданам и резидентам государств-членов, физическим и юридическим лицам. При введении института дополнительного гражданства Союза, без чего, как мы полагаем не обойтись на пути дальнейшего построения ЕАЭС, целесообразно закрепление единых цифровых прав и обязанностей за гражданами. Вместе с тем начать проработку и закрепление цифровых прав и обязанностей (подчеркнем, только в такой неразрывной связи, поскольку большие возможности цифровизации порождают и большие угрозы) можно уже сейчас на уровне Комиссии.

При проектировании Единого цифрового пространства необходимо закладывать возможность предоставления органами интеграции электронных услуг физическим и юридическим лицам. По аналогии с процессами G2B и G2Px (элементов электронного правительства) целесообразно создание цифровых коммуникаций в процедурах между органами интеграционного объединения и бизнесом, а также гражданами. Это значительно «приблизит» разноуровневых акторов интеграции, позволит сделать интеграционную систему мультисубъектной полицентричной сетевой моделью – наиболее эффективным типом построения социосистем в современном мире по М. Кастельсу.

Так, процедуры обращения заявителей в Суд ЕАЭС должны постепенно быть приведены к цифровому стандарту (например, направление электронными средствами связи любых процессуальных документов, использование электронной цифровой подписи) с поэтапным приведением к более сложным элементам электронного правосудия (например, создание электронных кабинетов и администрирование судопроизводства с использованием технологий, внедрение телекоммуникационных технологий на различных стадиях отправления правосудия). Эти и любые иные вопросы цифровизации деятельности органов ЕАЭС требуют тщательного планирования и правового обеспечения, начиная от включения соответствующих положений в акты первичного права Союза и заканчивая техническими правовыми актами.

Необходимо единообразное и в конечном итоге единое регулирование обращения данных в ЕАЭС. Министр по внутренним рынкам, информатизации, информационно-коммуникационным технологиям Евразийской экономической комиссии Г. Варданян в ходе панельной сессии «Цифровая повестка в Стратегии ЕАЭС до 2025 года», которая прошла в рамках цифрового форума в феврале 2021 г., сообщил, что необходимо определение четких подходов к разделению данных, ка-

кими целесообразно обмениваться в рамках интеграционных процессов, а какую информацию следует хранить исключительно в государстве-члене, а также выработать механизмы обеспечения безопасности данных (например, обезличивание), способных помочь расширить перечень видов информации для обмена. Оценивая это с юридической точки зрения, в рамках предусмотренной в настоящее время в Договоре компетенции Союза и государств-членов и возможных правовых инструментов взаимодействия это может быть сделано в форме международного договора в рамках Союза. В дальнейшем целесообразно отнесение этой компетенции в сферу единой политики и принятие соответствующего акта прямого действия обязательной юридической силы – например, решения ЕЭК.

Возвращаясь к тому, с чего начиналось данное исследование, а именно обозначению основного концепта любой успешной интеграции как свободы движения определенных факторов, к которым классически относят товары, услуги, капитал, трудовую силу и к которой в современную эпоху добавляется свобода движения информации, возможно сделать некоторое обобщение более высокого порядка: эффективная межгосударственная интеграция сопряжена со свободой движения ресурсов развития, и в предстоящей нам перспективе эти ресурсы во многом связаны именно с цифровой трансформацией, в том числе с созданием социо-цифровых сетей.

Выводы. Цифровая эпоха дает нам возможность «приблизить» интеграцию к многочисленному населению Евразийского экономического союза, сделать его институты понятными, создать действительно «пространство без границ» для торговли, общения, безопасности при сохранении национальной идентичности, суверенных прав. Расширение цифровой компетенции Союза актуально в областях, где правовое регулирование происходит в направлении унификации. Гармонизация информационного взаимодействия в иных сферах деятельности также необходима. Большие возможности цифровой эпохи порождают и вызовы в вопросах безопасности, этики, защищенности всех субъектов правоотношений. Это требует оперативного регулирования с привлечением экспертного потенциала на уровне Союза, а также схожих организационно-правовых механизмов реализации ответственности в случае нарушения установленных правил. Цифровая повестка ЕАЭС достаточно широкая, но и это лишь первые шаги на пути цифровой трансформации. Формирование прогнозной научно-обоснованной концепции развития Союза в цифровую эпоху сделает евразийский интеграционный проект эффективным, долгосрочным, устойчивым.

Список литературы

1. Большой Российский энциклопедический словарь. М.: Большая Российская энциклопедия; Дрофа, 2008. 1887 с.

2. Вельяминов Г. М. Международное право: опыты. М.: Статут, 2015. 1006 с.

3. Головенчик Г. Г. Цифровизация белоруской экономики в современных условиях цифровизации. Минск: Изд. Центр БГУ, 2019. 257 с.

4. Домрачев А. А., Евтушенко С. Н., Куприяновский В. П., Намиот Д. Е. Об инновационных инициативах государств-членов ЕАЭС в области построения глобаль-

ной цифровой экономики // International Journal of Open Information Technologies. – 2016. Vol. 4, № 9. С. 24–32.

5. Дорожная карта по цифровому сотрудничеству: осуществление рекомендаций Группы высокого уровня по цифровому сотрудничеству: доклад Генерального секретаря, 74-я сессия Генеральной Ассамблеи, 29 мая 2020 г. URL: https://undocs.org/ru/A/74/821 (дата обращения: 16.09.2022).

6. Зорькин В. Право в цифровом мире. Размышления на полях Петербургского международного юридического форума // Российская газета. 2018. 29 мая.

7. Казаков М. К. К вопросу о связи и отличиях информатизации и цифровизации // Актуальные проблемы социально-гуманитарного знания. 2019. С. 3–5.

8. Карлик А. Е., Платонов В. В., Кречко С. А. Организационное обеспечение цифровой трансформации кооперационных сетей и внедрения киберсоциальных систем // Научно-технические ведомости СПбГПУ. Экономические науки. 2019. Т. 12, № 5. С. 9–22.

9. Кастельс М. Информационная эпоха: экономика, общество, культура. М.: ГУ ВШЭ, 2000. – 608 с.

10. Михалева Т. Н. Правовое регулирование региональной экономической интеграции: вызовы и перспективы. Минск: Институт радиологии, 2016. 196 с.

11. Некрасов В. Н. Инновация, информатизация, цифровизация: соотношение и особенности правовой регламентации // Вопросы российского и международного права. 2018. № 8 (11А). С. 137–143.

12. Немирова Г. И., Виниченко А. А. Механизм повышения качества государственных услуг в области таможенного дела в условиях цифровой трансформации. М.: РИО Российской таможенной академии, 2017. 130 с.

13. Никулина Т. В., Стариченко Е. Б. Педагогическое образование в России // Информатизация и цифровизация образования: понятие, технологии, управление. 2008. № 8. С. 107–113.

14. Новиков А. Б. Рагозина Н. А. Правовое обеспечение создания единого информационного пространства Евразийского экономического союза (ЕАЭС) в сфере таможенного регулирования // Юридическая наука. 2018. № 6. С. 39–41.

15. Овчинников А. И. Тенденции развития права в условиях нового технологического уклада // Философия права. 2018. № 3 (86). С. 26–31.

16. Овчинников А. И., Фатхи В. И. Право и цифровая экономика: основные направления взаимодействия // Философия права. 2018. № (86). С. 128–134.

17. Прокудин Д. Е. От информатизации» к «цифровизации» Философская аналитика цифровой эпохи. СПб.: Изд-во Санкт-Петербургского университета, 2020. С. 38–52.

18. Саблина М. В. Проблемы информационного взаимодействия таможенных органов Евразийского экономического союза // Аллея науки. 2018. № 10. С. 715–718.

19. Саркисян Т. Цифровой суверенитет и цифровая повестка ЕАЭС. URL: https://eabr.org/press/news/tsifrovoy-suverenitet-i-tsifrovaya-povestka-eaes/ (дата обращения: 16.09.2022).

20. Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5–17.

21. Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9 (261). С. 5–16.

22. Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1 (253). С. 85–102.

23. Шабаева О. А. Право в условиях цифровой реальности: постановка проблемы // Сибирский юридический вестник. 2019. № 1 (84). С. 16–20.

24. Шафалович, А.А. Вызовы праву в эпоху цифровизации (на примере Республики Беларусь). Teisė, 2020. Vol. 114. С. 113–121. DOI: https://doi.org/10.15388/Teise.2020.114.7

25. Шугуров М. В. Тенденции и перспективы развития региональной научно-технологической интеграции в контексте цифровой повестки ЕАЭС: политико-правовое измерение // Право и политика. 2020. № 9. С. 119–141.

26. Паулин Алоис. Цифровизация против. Информатизация: разные подходы к трансформации управления // Центральная и Восточная Европа EDem и EGov Дни 331 (июль). – 2018. – Pp. 251–261. https://doi.org/10.24989/ocg.v331.21

27. Wagner B., Ferro C. Governance of Digitalisation in Europe: a Contribution to the Exploration Shaping Digital Policy – Towards a Fair Digital Society? Legal Notice. – 2020. – Bertelsmann Stiftung. – 49 p.

Р. В. Нигматуллин,
доктор юридических наук, профессор,
заведующий кафедрой международного права и международных отношений, заместитель директора по международной деятельности и связям с общественностью Института права,
Башкирский государственный университет

ЦИФРОВАЯ ДИПЛОМАТИЯ КАК ИНСТРУМЕНТ ВНЕШНЕЙ ПОЛИТИКИ

Аннотация. В XXI в. дипломатические отношения осуществляются с учетом новых реалий. Во взаимоотношениях государств стала внедряться публичная дипломатия, одной из составляющей которой является цифровая дипломатия. Сегодня в дипломатическом процессе участвуют граждане разных стран мира, опосредовано влияя на формирование внешнеполитического курса ведущих государств. Первостепенным направлением цифровой дипломатии стало общение с интернет-аудиторией. Присутствие в социальных сетях государственных деятелей, политиков, послов стало трендом текущего десятилетия. Российская цифровая дипломатия в сложной геополитической обстановке в мире позволяет оперативно распространять информацию о внешнеполитических инициативах России как среди зарубежной аудитории, так и российских граждан, используя возможности информационных каналов зарубежных стран и отечественных онлайн-платформ.

Ключевые слова: дипломатия, цифровизация, цифровая дипломатия, внешняя политика, цифровые технологии, российская цифровая дипломатия, информационно-коммуникационные технологии в дипломатии

DIGITAL DIPLOMACY AS A FOREIGN POLICY TOOL

Abstract. In the XXI century, diplomatic relations are carried out taking into account new realities. Public diplomacy, one of the components of which is digital diplomacy, has begun to be introduced into the relations of states. Today, citizens of different countries participate in the diplomatic process, indirectly influencing the formation of the foreign policy of the leading countries. The primary focus of digital diplomacy is to communicate with the Internet audience. The presence of state officials, politicians and ambassadors in social networks has become a trend of the current decade. Russian digital diplomacy in the complex geopolitical situation in the world allows for the rapid dissemination of information about Russia's foreign policy initiatives both to foreign audiences and to Russian citizens, using information channels of foreign countries and national online platforms.

Keywords: Diplomacy, Digitalization, Digital diplomacy, Foreign policy, Digital technologies, Russian digital diplomacy, Information and communication technologies in diplomacy

Введение. Развитие информационно-коммуникационных технологий открыло для человечества новые возможности в различных сферах жизни. Социально-политические процессы на планете стали проходить значительно быстрее, социальные сети как элемент информационных технологий стали оказывать на них глобальное как положительное, так и отрицательное влияние. Достаточно только упомянуть позитивные моменты, связанные с борьбой с COVID-19, и катастрофические последствия цветных революций и «арабской весны 2011 г.», в которых социальные сети сыграли роль катализатора и координатора.

XXI в. обоснованно называют цифровой эпохой. Новые возможности создали информационные технологии и в сфере международных отношений. В период пандемии в условиях закрытия границ международные саммиты и двусторонние контакты самого высокого уровня проводились онлайн с использованием IT-технологий. Дипломатические отношения стали осуществляться с учетом новых реалий. Онлайн-дипломатия стала постоянным атрибутом внешней политики. Многими государствами стала активно реализовываться цифровая дипломатия. Некоторые исследователи называют ее дипломатией будущего [5. С. 264–276]. Все это создало предпосылки вовлечения в дипломатический процесс огромного числа людей, что стало важным трендом современной эпохи.

Формирование подходов информационного обеспечения внешней политики. Развитые государства в последние десятилетия активно занимаются проблемой формирования и развития публичной дипломатии. Ее составляющими стали международное гуманитарное сотрудничество, сотрудничество государств в образовательной сфере, экспертная дипломатия, а также цифровая дипломатия.

Также в качестве составляющих публичной дипломатии российские исследователи отмечают «работу с соотечественниками, тематику сохранения исторической правды и политику противодействия фальсификации истории в международном общественном пространстве, цифровую дипломатию (Facebook- и Twitter-дипломатия (Facebook, Twitter – признанные экстремистскими социальные сети, запрещенные в Российской Федерации)), внешние зарубежные связи Русской Православной Церкви, международное сотрудничество регионов и городов-побратимов» [16. С. 12].

Пионером в развитии цифровой дипломатии выступили США. В короткий срок она стала элементом государственной политики. Как отмечает И. В. Сурма, внедрение элементов цифровой дипломатии в США фактически началось в конце 90-х гг. XX в. и получило окончательное оформление, став направлением программы «Государственное управление в XXI веке» в 2009 г. при Государственном секретаре США Хилари Клинтон [12. С. 222–223].

Аналогичного мнения придерживается Н.А. Цветкова, которая отмечает, что «цифровая дипломатия как правительственный механизм влияния на пользователей социальных сетей появилась в системе международных отношений примерно в 2009–2010 гг., когда государственные структуры таких стран, как США, Россия, Франция, Германия, Китай и Иран, приступили к созданию официальных учетных профилей (аккаунтов) на платформах Facebook, Twitter (Facebook, Twitter запрещенны в Российской Федерации), YouTube и др., а международные медийные компании, включая Voice of America, Russia Today и PressTV, запустили первые цифровые каналы вещания в социальных сетях» [15. С. 38–39]. Это явилось результатом понимания государством возможности влияния на огромные массы людей в целях реализации задач, обеспечивающих, в первую очередь, интересы национальной безопасности. Возможности социальных сетей изначально были восприняты как новые элементы понятия «мягкая сила».

Проблема публичной дипломатии в Российской Федерации получила громкое звучание в начале 2000-х гг. Это было связано с постановкой соответствующих задач в Концепции внешней политики Российской Федерации 2000 г., где в частности говорится о необходимости ускоренного развития в Российской Федерации собственных эффективных средств информационного влияния на общественное мнение за рубежом [7]. Следующим сигналом о необходимости внимательного отношения к этому направлению работы стало выступление Президента России В. В. Путина 12 июля 2004 г. на пленарном заседании совещания послов и постоянных представителей России, где он заявил, что представления о России в мире очень часто далеки от реальности, и «посольства и другие зарубежные представительства должны принять активное участие в формировании непредвзятого благоприятного представления о внутренней и внешней политике Российской Федерации, о ее истории, о ее культуре, о сегодняшнем развитии» [4].

В дальнейшем, в концепциях внешней политики 2013 г. и 2016 г. задача поступательного информационного обеспечения внутренней и внешней политики России получала дальнейшее развитие. Обобщенно, в качестве главного направления ее реализации можно выделить распространение объективной и всесторонней информации о внешней политике России.

Решение этой задачи предполагает широкое использование возможностей цифровой дипломатии. Цифровая дипломатия имеет много определений и большинство из них подчеркивают применение социальных сетей для распространения среди граждан зарубежных стран позиции государства по тем или иным вопросам внешнеполитической повестки.

Форсированной цифровизации всех аспектов жизни человечества, в том числе и дипломатии, способствовала пандемия COVID-19.

Социальные сети как основа цифровой дипломатии России. Многие страны мира стали обращать внимание на то, что цифровизация расширила возможности доведения целей своей внешней политики до руководства и населения иностранных государств. При этом необходимо отметить, что одним из преимуществ цифровой дипломатии является «мягкое» воздействие цифрового инструментария внешнеполитической деятельности, что позволяет добиться ненавязчивого распространения государственных интересов по всему миру [8. С. 104]. То есть, одной из важнейших целей цифровой дипломатии является обоснование перед зарубежной и внутренней аудиторией верности принятия внешнеполитических решений.

Первостепенным направлением цифровой дипломатии стало общение с интернет-аудиторией, которая в XXI в. значительно увеличилась, включив в себя и малограмотное население планеты. Присутствие в социальных сетях государственных деятелей, политиков, послов стало трендом текущего десятилетия. В мировых социальных сетях, таких как «Фейсбук», «Твиттер», «Инстаграм» (признаны экстремистскими и запрещены в Российской Федерации), «Ютуб» появились аккаунты также внешнеполитических ведомств и дипломатических представительств и всевозможных фондов, советов так или иначе участвующих в позиционировании деятельности государства за рубежом.

Согласно докладу «Twiplomacy Study 2018», русскоязычный Твиттер-аккаунт МИД России стал пятым по числу подписчиков (после США, Саудовской Аравии, Индии и Турции). По размеру сети дипломатических аккаунтов МИД России с 244 аккаунтами занял второе место после Великобритании (413 аккаунтов), опережая Государственный департамент США, постпредство России при ООН вошло в топ-7 миссий с более чем 250 взаимными подписками с другими представительствами и дипломатами (первые два места достались США) [16, с. 38]. Этому поспособствовало, по-видимому, то, что при использовании мировых социальных сетей для распространения информации о внешней политике государства был осуществлен иной подход в подаче материала. Как отмечает И. В. Сурма, успех аккаунта МИД России в «Фейсбуке» (признана экстремистской и запрещена в РФ) во многом был предопределен подачей материала, представляющего «три группы: во-первых, это официальные сообщения министерства; во-вторых, сопутствующие материалы, относящиеся к истории российской дипломатии или к актуальным международным событиям; и, в-третьих, сообщения с ироничным или откровенно юмористическим наполнением, внезапными цитатами, смелыми заголовками» [12. С. 229].

Необходимо отметить большую работу по «цифровизации» российской дипломатии, с 2018 г. МИД России и дипломатические представительства России стали создавать аккаунты в социальной сети «ВКонтакте».

В 2019 г. количество уникальных подписчиков аккаунта Министерства иностранных дел России «в «Фейсбуке» достигло 384 тыс. (на английском и русском языке), на арабском аккаунте – 2 тыс. В «Твиттере» на русском языке – 1,2 млн, на английском – 227 тыс., на испанском – 11 тыс., на арабском – 15 тыс. … В сети «ВКонтакте» – 402 тыс.; в «Инстаграме» – 227 тыс.; в «Перископе» – 78 тыс.; на «Ютубе» – 20 тыс.». [9. С, 134] (Facebook, Twitter, Instagram – признанные экстремистскими социальные сети, запрещенные в Российской Федерации).

В 2020 г. количество уникальных подписчиков аккаунта в «Твиттере» на русском языке составило 1,1 млн, на английском – 273 тыс., на испанском – 20,5 тыс., на арабском – 31,5 тыс.; в «Фейсбуке» – 448 тыс.; в сети «ВКонтакте» – 408 тыс.; в «Инстаграме» – 361 тыс.; в «Ютубе» – 25 тыс.; в мессенджере «Вайбер» – 5,5 тыс.; в «Телеграм» – 13 тыс. На Интернет-сайте МИД России было опубликовано 2 363 материала по актуальным внешнеполитическим проблемам (на русском и иностранных языках) [10. С. 62–63] (Facebook, Twitter, Instagram – признанные экстремистскими социальные сети, запрещенные в Российской Федерации).

В докладе Российского совета по международным делам «Публичная дипломатия России в эпоху COVID-19. Ежегодный обзор основных трендов и событий публичной дипломатии России в 2020 году» отмечается, что «именно 2020 г. стал годом резкого скачка и развития одного из важнейших компонентов системы публичной дипломатии – информационного направления публичной дипломатии, а именно – цифровой дипломатии, к которому относится работа. в том числе в социальных сетях» [2. С. 5]. Вместе с тем, необходимо признать, что развитие цифровой дипломатии прошло через определенные этапы, обусловленные как развитием публичной дипломатии, так и совершенствованием IT-технологий. Сейчас больше обращается внимание на повышение качества работы в сфере цифровой дипломатии. Для этих целей стали использоваться возможности искусственного интеллекта. На практике уже применяется так называемая дипломатия данных (data diplomacy), которая позволяет специалистам формировать стратегии цифровой дипломатии, составлять эффективные посты, месседжи и мгновенно определять источники дезинформации [15. С. 45].

Российское внешнеполитическое ведомство демонстрирует серьезную активность в социальных сетях. Стала регулярной информация о телефонных разговорах Президента России В. В. Путина с Генеральным секретарем ООН и главами зарубежных государств, о встречах Президента России В. В. Путина с главами зарубежных государств, о пресс-конференциях Президента России В .В. Путина по итогам зарубежных визитов или участии в международных саммитах, поздравления граждан других стран с государственными и национальными праздниками, выступления, интервью, ответы СМИ и «на полях» саммитов министра иностранных дел России С. В. Лаврова, пресс-конференции заместителей министра иностранных дел России по различным аспектам международной повестки, интервью директоров департаментов МИД России, заявления МИД России в связи с международными событиями, брифинги официального представителя МИД России М.В. Захаровой по текущим вопросам внешней политики, выступления и ответы Постоянного представителя России при ООН и в Совете Безопасности ООН В. А. Небензи.

Аккаунты появились у структурных подразделений министерства, 286 посольств и консульских учреждений, 11 постоянных представительств, 43 территориальных представительствах [1]. Наблюдается и персонализация цифровой дипломатии. Как отмечает О. А. Мельникова, «некоторые представители Министерства из числа высшего руководства имеют персональные страницы, где также ведется активное обсуждение вопросов по международной проблематике» [9, с. 135]. Аккаунты имеют первый заместитель Постоянного представителя России при ООН Д. А. Полянский, Постоянный представитель России при Отделении ООН и других международных организациях в Женеве Г. М. Гатилов, Постоянный представитель России при международных организациях в Вене М. И. Ульянов, Уполномоченный МИД России по вопросам прав человека демократии и верховенства права Г. Е. Лукьянцев, Посол России на Мадагаскаре С. А. Ахмедов, Посол России в Камбодже А. В. Боровик, Посол России в Австрии Д. Е. Любинский и другие [1].

Сегодня цифровая дипломатия используется и в повседневной деятельности дипломатических представительств и консульских учреждений. Информация посольств, как правило, либо посвящена их деятельности и в связи с этим может быть интересна читателю, либо пропагандирует достижения своей страны через призму международных отношений. Важной, оказывающей помощь нашим гражданам, представляется информация посольств и консульств об изменении работы консульских отделов, изменении сроков рассмотрения заявлений на получение виз, об изменениях расписания рейсов самолетов, прилетающих и вылетающих из страны аккредитования. В контексте работы по преодолению последствий пандемии коронавируса на веб-портале МИД России были созданы специальные разделы, посвященные усилиям российских дипломатических и консульских учреждений по содействию вывозу граждан России из-за рубежа, публиковалась полезная информация по порядку въезда в Российскую Федерацию и выезда из страны [10. С. 62–63]. Российские дипломатические представительства и консульские учреждения через социальные сети направляют на мобильные телефоны российским гражданам, находящимся за рубежом, сообщения о пересечении административных границ стран Европейского союза и телефонах посольств и консульств в стране пребывания, а также о возникновении чрезвычайных ситуаций.

Однако в настоящий момент деятельность российского внешнеполитического ведомства по размещению информации в мировых социальных сетях затруднилась. Администрации социальных сетей стали удалять материалы официальных представителей России, объясняющие действия страны в различных сферах жизни. Так, 16 августа 2022 г. Посольство России в Великобритании выступило с комментарием в связи с враждебными действиями видеохостинга «Ютуб»: «15 августа администрация видеохостинга «Ютуб» без предупреждения удалила с канала Посольства в общей сложности 29 видеоматериалов. Большинство из них составляют интервью Посла России в Великобритании А. В. Келина (за период с 2 марта по 15 августа с. г.). Данные интервью охватывают широкую проблематику: российско-британские отношения, глобальный продовольственный и энергетический кризис, положение соотечественников за рубежом, неправомерная санкционная

политика западных стран, а также разъяснения целей и задач специальной военной операции России на Украине» [6].

Посольство России обратило внимание администрации «Ютуба» на то, что в действиях видеохостинга усматриваются признаки нарушения принципов и обязательств ОБСЕ, касающихся свободы выражения мнения и средств массовой информации, которые взяли на себя все государства-участники, включая Великобританию [6].

После начала 24 февраля 2022 г. специальной военной операции России в поддержку ДНР и ЛНР в социальных сетях началась откровенная антироссийская компания. Под репрессии западных государств попали крупные отечественные СМИ, освещавшие на протяжении многих лет международные новости, а также их руководители и рядовые сотрудники. Затем последовала активная блокировка российских информационных ресурсов на мировых онлайн-платформах. В частности, по этому поводу министр иностранных дел России С. В. Лавров в своем выступлении на международной научно-практической конференции «Цифровые международные отношения 2022» отметил: «Необоснованные рестрикции накладываются на публикации МИД России и загранучреждений в сети «Твиттер» только за то, что мы говорим правду и подкрепляем свои слова фактами» [3].

4 марта 2022 г. в России был заблокирован «Фейсбук», а 21 марта – «Инстаграм». Это стало ответом на решение руководства компании Meta Platforms Ins. временно снять в своих социальных сетях «запрет для жителей ряда стран на размещение информации, содержащей призывы к насилию в отношении российских граждан, в том числе военнослужащих» [13]. Тверской суд Москвы 21 марта признал деятельность «Фейсбук» и «Инстаграм» экстремистской и запретил их на территории России.

Сегодня популярной социальной сетью, которую используют МИД России, посольства Российской Федерации и иностранные посольства стала «ВКонтакте». Посольства России в зарубежных странах в настоящее время в этой сети предоставляют гражданам страны пребывания широкий спектр информационных материалов. Это поздравления Президента России по случаю важных событий, включая установление дипломатических отношений; информация о переговорах; комментарии официального представителя МИД России М.В. Захаровой; комментарии посольства по актуальным вопросам межгосударственных отношений; выступления и встречи послов России в стране пребывания; информация о культурных и исторических объектах нашей страны. Так, 20 августа 2022 г. Посольство России в США дало комментарий на запрос издания Newsweek по ситуации с контролем над вооружениями. Регулярно дается информация по студенческому обмену. В 2022 г. количество уникальных подписчиков аккаунта Министерства иностранных дел России в сети «ВКонтакте» превысило 451 тыс., в «Телеграм» на русском языке стало более 115 тыс. подписчиков, на английском – более 33 тыс., на испанском – 6,5 тыс.

В социальной сети «Вконтакте» активно размещают свою информацию дипломатические представительства зарубежных государств, аккредитованные в России. Как правило, эти материалы посвящены популяризации историко-культурных достопримечательностей страны, а зачастую направлены на пропаганду

преимуществ работы и обучения. Так, посольство Японии 21 января 2022 г. объявило о начале приема документов на программу обмена и обучения на 2022 г. на позицию координатора международных связей.

Посольство Великобритании 16 августа 2022 г. разместило информацию о том, что британский паспорт занял шестое место в рейтинге Henley Passport Index, и теперь граждане Великобритании могут посещать 187 государств без виз, 19 августа – о реконструкции Музея Лондона.

Посольство КНР уделяет много внимания достижениям Китая в области экономики, науки и социальной сферы. Значительное место занимают китайско-российские отношения, популяризация художественно-природных достопримечательностей. Так, 16 августа 2022 г. посольство опубликовало подробную информацию о Топ-10 музеев Китая, которые рекомендуется посетить в силу художественной и исторической ценности представленных материалов.

5 сентября 2022 г. Президент России своим указом утвердил Концепцию гуманитарной политики Российской Федерации за рубежом. В соответствии с документом на МИД России возлагается реализация внешнеполитического курса в сфере гуманитарной политики, координация деятельности федеральных органов исполнительной власти и международных связей субъектов Российской Федерации. На наш взгляд, важным и требующим серьезного внимания, является положение концепции о необходимости комплексного подхода к информационному сопровождению всех значимых событий, происходящих в нашей стране, и международных мероприятий с ее участием [14].

Достаточно полно в концепции обозначены основные направления гуманитарной политики. Это, в частности, традиционные ценности, помощь государствам, пострадавшим от стихийных бедствий, техногенных катастроф и террористических актов, продвижение русского языка в качестве языка международного общения, продвижение за рубежом достижений культуры, науки, образования.

Очень много внимания в концепции уделено использованию Интернета и социальных сетей для достижения целей и задач гуманитарной политики. Предполагается широкое внедрение современных цифровых технологий. Продвижение за рубежом отечественных цифровых образовательных платформ и социальных сетей существенно повысит эффективность инструментов российской «цифровой дипломатии» [14]. Отмечается, что СМИ, социальные сети, мессенджеры и блоги являются наиболее эффективным инструментом «мягкой силы».

Вместе с тем необходимо отметить, что цифровая дипломатия России подвержена и определенным угрозам. В качестве наиболее опасных отмечаем: во-первых, противодействие «коллективного запада» путем блокирования российских аккаунтов в подконтрольных социальных сетях; во-вторых, использование информационно-коммуникационных технологий в целях дискредитации российской внешней политики. Тем не менее, эти угрозы находятся в поле зрения России, и государством предпринимаются соответствующие шаги по противодействию. Так, с 29 августа по 9 сентября состоялась третья сессия Специального межправительственного комитета ООН (Спецкомитета) по разработке всеобъемлющей международной конвенции по противодействию использованию информационно-коммуникационных

технологий в преступных целях, учрежденного по инициативе России при соавторстве 46 государств резолюцией Генеральной Ассамблеи ООН 74/247. По итогам сессии было решено подготовить консолидированный «нулевой» проект будущего международно-правового договора, который будет рассмотрен государствами-членами в ходе четвертой и пятой сессий Спецкомитета (состоятся соответственно в Вене 9–20 января и 11–23 апреля 2023 г.). Итоговый текст конвенции планируется представить Генеральной Ассамблее ООН в ходе ее 78-й сессии в 2024 г. [11].

Заключение. Сегодня цифровая дипломатия стала важным фактором обеспечения внешнеполитических интересов страны. В свою очередь, в условиях усложнения международных отношений в мире она позволяет оперативно информировать как зарубежную аудиторию, так и российских граждан о внешнеполитических инициативах России, ее позиции по важнейшим проблемам обеспечения международной безопасности, используя в рамках законодательства России возможности информационных каналов зарубежных стран и отечественных онлайн-платформ. Российская цифровая дипломатия активно развивается в этом направлении, уделяя большое внимание совершенствованию информационно-коммуникационных технологий и цифровых продуктов, в том числе путем сотрудничества с отечественными научными организациями и центрами. В настоящее время готовится новая концепция внешней политики Российской Федерации. На наш взгляд, она должна ответить и на новые вызовы в сфере информационного сопровождения внешнеполитической деятельности Российской Федерации. В частности, предусмотреть целенаправленное противодействие попыткам фальсификации истории, современности и роли России в международных делах, в том числе и с использованием возможностей социальных сетей; популяризацию имеющего всемирное значение культурного, исторического и природного потенциала России в целях усиления авторитета России на международной арене.

Список литературы

1. Аккаунты в соцсетях // Министерство иностранных дел Российской Федерации. URL: http://www.mid.ru/ru/press_service/social_accounts (дата обращения: 30.08.2022).

2. Бурлинова Н. Публичная дипломатия России в эпоху COVID-19. Ежегодный обзор основных трендов и событий публичной дипломатии России в 2020 г.: доклад Российского совета по междунар. делам (РСМД), доклад № 71/2021 / Н. Бурлинова, М. Чагина, В. Иванченко; Российский совет по междунар. делам (РСМД), Центр поддержки и развития общественных инициатив «Креативная дипломатия». – М.: НП РСМД, 2021. 36 с.

3. Выступление Министра иностранных дел Российской Федерации С. В. Лаврова на пленарной сессии «Международные отношения в условиях цифровизации общественной жизни» международной научно-практической конференции «Цифровые международные отношения 2022», Москва, 14 апреля 2022 года // Министерство иностранных дел Российской Федерации. URL: https: // www.mid.ru/ru/foreign_policy/news/1809294/ (дата обращения: 15.09.2022).

4. Выступление Президента России В.В. Путина на пленарном заседании совещания послов и постоянных представителей России, Москва, министерство иностранных дел, 12 июля 2004 года // Официальный сайт МИД РФ. URL: https://www.mid.ru/ru/foreign_policy/news/1745717/ (дата обращения: 26.08.2022).

5. Заемский В.Ф., Карпович О.Г. Цифровая дипломатия – дипломатия будущего // Дипломатическая служба. 2021. № 3. С. 264–276.

6. Комментарий Посольства России в Великобритании в связи с враждебными действиями видеохостинга «Ютуб», 16 августа 2022 года // Официальный сайт Посольства России в Великобритании. URL: https://www.rus.rusemb.org.uk/fnapr/6292. (дата обращения: 20.08.2022).

7. Концепции внешней политики Российской Федерации 2000 года // Электронный фонд правовых и научно-технических документов. URL: https://docs.cntd.ru/document/901764263?ysclid=l8a074v7go510834551. (дата обращения: 19.09.2022).

8. Лебедева О. Современные инструменты «цифровой дипломатии» как важнейший элемент «мягкой силы» // Международная жизнь. Май 2019. С. 102–111.

9. Мельникова О. А. Информационное обеспечение внешнеполитической деятельности современных государств (политологический анализ): диссертация на соискание ученой степени кандидата политических наук. Москва, 2022. 210 с.

10. Обзор МИД России: «Внешнеполитическая и дипломатическая деятельность Российской Федерации в 2020 году». 66 с. URL: http:// https://www.mid.ru/ru/activity/review (дата обращения: 30.08.2022).

11. О сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности // Официальный сайт МИД РФ. URL: https://mid.ru/ru/foreign_policy/news/1829389/ (дата обращения: 19.09.2022).

12. Сурма И.В. Цифровая дипломатия в мировой политике // Государственное управление. Электронный вестник. Апрель 2015. № 49. С. 220–249.

13. Суд запретил Instagram и Facebook. Что это значит для пользователей. URL: https://www.rbc.ru/technology_and_media/21/03/2022/6238a5e89a79477e5dc0245f. (дата обращения: 20.08.2022).

14. Указ Президента Российской Федерации «Об утверждении Концепции гуманитарной политики Российской Федерации за рубежом» // Официально интернет-представительство президента России. URL: http://static.kremlin.ru/media/events/files/ru/G3CkAuMhZXio8AzNaweT3wTGTaEA16OU.pdf (дата обращения: 19.09.2022).

15. Цветкова Н.А. Феномен цифровой дипломатии в международных отношениях и методология его изучения // Вестник РГГУ. Серия «Политология. История. Международные отношения». 2020. № 2. С. 37–47. DOI: 10.28995/2073-6339-2020-2-37-47

16. Экспертный обзор российской публичной дипломатии в 2018–2019 гг. 10 шагов на пути к эффективной публичной дипломатии России: доклад 52/2020 / [Н. Бурлинова, П. Василенко, В. Иванченко, О. Шакиров]; [вып. ред. И. Тимофеев, О. Пылова]; Российский совет по международным делам (РСМД). Москва: НП РСМД, 2020. – 58 с.

Ю. А. Соловьева,
кандидат юридических наук,
доцент кафедры конституционного и международного права,
Донецкий национальный университет

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВОЙ ЭКОНОМИКИ

Аннотация. В статье рассмотрены основные особенности международно-правового регулирования цифровой экономики; отмечено, что на первоначальном этапе развития цифровых технологий объектами международно-правового регулирования были принципы и направления развития последних в основных сферах общественной жизни (в том числе экономике), а в последующем возникла необходимость в разработке механизмов противодействия кибернарушениям, чтобы использование общественно полезных преимуществ цифровизации «не было зачеркнуто» ее рисками.

Ключевые слова: цифровые технологии, цифровизация, цифровая экономика, информационное общество, правовое регулирование, киберправонарушения, киберпреступления

INTERNATIONAL LEGAL REGULATION OF THE DIGITAL ECONOMY

Abstract. The article considers the main features of the international legal regulation of the digital economy; noted that at the initial stage of development of digital technologies, the objects of international legal regulation were the principles and directions of development of the latter in the main areas of public life (including the economy), and subsequently it became necessary to develop mechanisms to counteract cyber violations in order to use the socially beneficial advantages of digitalization «was not crossed out» by its risks.

Keywords: Digital technologies, Digitalization, Digital economy, Information society, Legal regulation, Cyber offenses, Cyber crimes

Сегодня в Российской Федерации внедряются реформы во многих сферах общественной жизни. Основные направления изменений отражены в Указе Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.» [1], где были определены цели, задачи и меры по реализации внутренней и внешней политики России в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов. В данной Стратегии также делается акцент на том, что в сегодняшних реалиях, когда не установлены международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, ряду стран необходимо «на бегу» адаптировать государственное регулирование сферы информационных технологий к новым обстоятельствам.

В связи с чем целью данного исследования является освещение вопросов международно-правового регулирования цифровой экономики.

Безапелляционно, что возникновение цифровой экономики стало следствием стремительного развития цифровых технологий, правовое обеспечение которых сегодня является актуальным как для каждого отдельного государства, так и для всего мирового сообщества. Цифровая экономика стала одним из элементов информационного общества, регулирование которого на международном уровне началось с принятия в 2000 г. Окинавской хартии глобального информационного общества Организации Объединенных Наций (далее – ООН) [2], которой указывалось, что внедрение современных информационных технологий осуществляет свое влияние на экономику стран, образ жизни людей и социальное развитие, взаимодействие государственных структур и населения. В связи с чем каждому государству необходимо акцентировать внимание на следующих ключевых направлениях развития информационных технологий: 1) внедрение и реализация экономических реформ для повышения эффективности и открытости государственного управления; 2) осуществление рационального управления макроэкономикой с использованием преимущества информационных технологий; 3) разработка и внедрение информационных сетей для быстрого, надежного, безопасного и экономичного доступа к сетевым технологиям, их обслуживанию и применению; 4) развитие информационного общества, в котором каждое лицо имеет возможность иметь доступ к образованию в сфере информационных технологий; 5) широкое использование информационных технологий в государственном секторе, развитие форм взаимодействия граждан и организаций с органами государственной власти.

Также в декабре 2003 г. ООН была принята Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» [3], призванную сформулировать и закрепить основные принципы построения информационного общества, среди которых, в частности, следующие: 1) построение информационного общества, в котором были бы обеспечены созданные государством условия для взаимодействия интересов личности и государства, внедрен принцип взаимной ответственности; 2) обеспечение доступа населению к информационно-коммуникационным технологиям; 3) обеспечение открытости информационного общества; 4) создание условий, при которых каждый человек мог бы овладеть знаниями, необходимыми для понимания сути информационного общества, и использовать их в сфере экономики; 5) создание механизмов защиты информационного пространства с целью повышения роста доверия населения к информационным технологиям и пр.

Позднее, в 2005 г., в поддержку указанной декларации был принят План действий Тунисского обязательства [6], в котором были разработаны механизмы для решения актуальных проблем развития информационно-коммуникационных технологий.

Таким образом, данные международные акты заложили основу международно-правового регулирования цифровой экономики. В них делался акцент на необходимости информатизации различных сфер общественных отношений (особенно экономической); закреплялись принципы, в строгом соответствии с которыми такая информатизация должна происходить. В то же время в каждом из них обращалось

внимание на то, что информатизация общества в глобальном пространстве приводит к росту кибервызовов и угроз, включая киберпреступность как один из новейших феноменов теневой экономики. Именно по этой причине в последующем в международных актах, регулирующих различные вопросы цифровизации экономики, все чаще имело место закрепление механизмов противодействия угрозам, обусловленным оборотом значительных массивов информации в связи с предоставлением электронных услуг, электронной торговли и пр.

Так, например, в 2014 г. Европейским парламентом был принят Регламент № 910/2014 об услугах электронной идентификации и укрепления доверия для электронных транзакций на внутреннем рынке и отмены Директивы 1999/93 / ЕС [7], целью разработки которого было повышение уровня доверия к электронным транзакциям на внутреннем рынке путем создания общей основы для безопасного электронного взаимодействия между гражданами, субъектами предпринимательской деятельности и органами публичной власти, улучшая, таким образом, действенность публичных и частных онлайн-услуг, электронного бизнеса и электронной коммерции в Союзе. В то же время для обеспечения надлежащего функционирования внутреннего рынка и достижения надлежащего уровня безопасности средств электронной идентификации и доверительных услуг данным Регламентом было установлено следующее: 1) условия, на которых государства-члены признают средства электронной идентификации физических и юридических лиц, охватываемых нотифицированной схемой электронной идентификации другого государства-члена; 2) правила по доверительным услугам, в частности, по электронным транзакциям; 3) правовые рамки для электронных подписей, электронных печатей, электронных меток времени, электронных документов, услуг регистрируемой электронной доставки и услуг по предоставлению сертификатов для проверки подлинности веб-сайтов.

Важно заметить, что на необходимости создания институтов и процедур, направленных на решение проблем цифровой безопасности и защиты от кибератак, борьбу с киберпреступностью и повышение общего доверия населения к цифровым экосистемам, которые лежат в основе цифровой экономики, акцентируется внимание и в Цифровой повестке Евразийского экономического союза (далее – ЕАЭС) до 2025 г. [8]. Данной повесткой также обозначается необходимость согласования и утверждения обязательных требований по обеспечению кибербезопасности в странах ЕАЭС, плана действий по обеспечению кибербезопасности на уровне Союза и пр.

Наряду с этим вопросы создания системы, обеспечивающей международную информационную безопасность в сфере экономики стали частым предметом обсуждения на различных международных форумах, например Шанхайской организации сотрудничества (далее – ШОС), «Группы двадцати» и пр. Так, членами ШОС было отмечено, что стимулирование информационно-технологического сектора является безоговорочным императивом для экономического развития каждой страны-участницы, но, с другой стороны, необходимо не допускать использования современных информационных технологий для оказания деструктивного воздействия на государственную целостность, стабильность и национальную безопасность стран ШОС [9]. Этот признанный факт стал причиной последующего подписания

в 2009 г. Соглашения «О сотрудничестве в области обеспечения международной информационной безопасности» [10].

Позднее, на саммите G 20 в 2014 г., лидерами стран был поддержан тезис о том, что угрозы безопасности использования информационно-коммуникационных технологий рискуют подорвать коллективную способность применять Интернет для стимулирования экономического роста и развития во всем мире [11. С. 21].

В контексте обозначенного хотелось бы заметить, что на 56-й сессии Генеральной Ассамблеи ООН была принята консенсусом резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» A/RES/56/19, предложенная РФ [12]. В тексте документа указывалось, что «Генеральная Ассамблея ООН… просит Генерального секретаря рассмотреть существующие и потенциальные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению…». В п. 3 данной резолюции указывалось также, что все государства-члены обязаны продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, информировать Генерального секретаря о своей точке зрения и об оценках по ряду вопросов, а именно: 1) общей оценки проблем информационной безопасности; 2) усилий, предпринимаемых на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области; 3) возможных мерах, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне.

Необходимо также отметить, что дальнейшее развитие цифровой экономики в мире привело к появлению новых элементов, нуждающихся в надлежащем правовом регулировании, например, интернета вещей, криптовалюты, больших данных, цифровых технологических платформ и пр. В качестве примера можно привести Директиву ЕС 2009/110/ЕС, регулирующую вопросы эмиссии электронных денег [13], Рекомендацию Международного союза электросвязи МСЭ-Т Y.2069 «Серия Y: Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений. Сети последующих поколений – структура и функциональные модели архитектуры. Термины и определения для интернета вещей» [14] и пр.

Заключение. Таким образом, проведенное исследование позволяет сделать ряд выводов.

Во-первых, цифровизация экономики происходит уже более двадцати лет. При этом если на первоначальном этапе объектом международно-правового регулирования были принципы и направления развития цифровых технологий в основных сферах общественной жизни (в том числе экономике), то в последующем возникла необходимость в разработке механизмов противодействия кибернарушениям и киберпреступлениям, чтобы использование общественно полезных преимуществ цифровизации «не было зачеркнуто» ее рисками (что нашло отражение в международных нормах).

Во-вторых, дальнейшее развитие цифровой экономики в мире привело к появлению новых элементов, нуждающихся в надлежащем правовом регулировании,

например, интернета вещей, криптовалюты, больших данных, цифровых технологических платформ и пр.

В-третьих, сегодня международно-правовое регулирование процессов цифровизации экономики преследует следующие основные цели: формулирование основных понятий и терминов, обозначивших соответствующие процессы; определение правового режима использования цифровых технологий в сфере экономики; обеспечение защиты информационных прав человека и соответственно предупреждение возможности кибернарушений.

Список литературы

1. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203 // Сайт Президента России. URL: http://kremlin.ru/acts/bank/41919 (дата обращения: 27.07.2022).

2. Окинавская Хартия глобального информационного общества (подписана 22 июля 2000 года лидерами стран «Большой восьмерки»). URL: https://libre.life/doc/charta/ru (дата обращения: 27.07.2022).

3. Декларация принципов (построение информационного общества – глобальная задача в новом тысячелетии) // Межрегиональный центр библиотечного сотрудничества. URL: http://www.mcbs.ru/documents_20/5/45/ (дата обращения: 27.07.2022).

4. Тунисская программа для информационного общества. URL: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения: 27.07.2022).

5. Регламент (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 года об услугах электронной идентификации и укрепления доверия для электронных транзакций на внутреннем рынке и отмены Директивы 1999/93 / ЕС. URL: https://mytocz.eu/ru/etoll/legislation (дата обращения: 27.07.2022).

6. Цифровая повестка Евразийского экономического союза до 2025 года: перспективы и рекомендации. URL: https://eec.eaeunion.org/upload/directions_files/a34/a34a8a322ff61b3e9fba79b3006213c0.pdf (дата обращения: 27.07.2022).

7. Чумаченко Т. Н. Деятельность ШОС по обеспечению международной информационной безопасности // Вестник КазНПУ. 2017. URL: https://articlekz.com/article/18976 (дата обращения: 27.07.2022).

8. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. URL: https://lex.uz/docs/2068478 (дата обращения: 27.07.2022).

9. Дж. Киртон, Б. Уоррен Повестка дня «Группы двадцати» в области цифровизации // Вестник международных организаций. 2018. Т. 13, № 2. С. 17–47.

10. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Доклад Генерального секретаря (документ A/RES/53/70). URL: https://undocs.org/pdf?symbol=ru/a/73/505 (дата обращения: 27.07.2022).

11. Директива Совета Европейских сообществ 2009/110/ЕС от 16 сентября 2009 г. об учреждении и деятельности организаций, эмитирующих электронные деньги, о пруденциальном надзоре за их деятельностью, а также об изменении

Директив 2005/60/ЕС и 2006/48/ЕС и об отмене Директивы 2000/46/ЕС. URL: https://base.garant.ru/71312234/ (дата обращения: 27.07.2022).

12. Рекомендация Международного союза электросвязи МСЭ-Т Y.2069. Серия Y: Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений. Сети последующих поколений – структура и функциональные модели архитектуры. Термины и определения для интернета вещей. URL: https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-Y.2069–201207-I!!PDF-R&type=items (дата обращения: 27.07.2022).

В. М. Шумилов,
доктор юридических наук, профессор,
Всероссийская академия внешней торговли
Министерства экономического развития России

МЕЖДУНАРОДНОЕ ЦИФРОВОЕ ПРАВО КАК ОТРАСЛЬ МЕЖДУНАРОДНОГО ПРАВА

Аннотация. Цель статьи – донести авторский взгляд на появление и развитие в международной системе относительно новой правовой реальности – международного цифрового права. Раскрывается вопрос о качественном состоянии данного нормативного блока, о его предмете и месте в системе международного права. Обращено внимание на терминологическую проблему и на соотношение международного права и национальных правовых систем в том, что касается деятельности в электронном пространстве как частных лиц, так и самих государств и международных организаций. Делается вывод о том, что «международное цифровое право» такая же реальность, как и регулируемое им транснациональное электронное пространство, только право, как это часто бывает, отстает от нужд регулирования. Международное цифровое право – это еще только формирующаяся отрасль международного права.

Ключевые слова: цифровое право, международное цифровое право, международное право, внутреннее (национальное) право, отрасль международного права, международная система, трансформация международной системы

INTERNATIONAL DIGITAL LAW AS A BRANCH OF INTERNATIONAL LAW

Abstract. The purpose of the article is to convey the author's view on the emergence and development of a relatively new legal reality in the international system: "international digital law". The question of the quality of this normative block, its subject and place in the system of international law is revealed. Attention is drawn to the terminological problem and the correlation of international law and national legal systems in terms of the activities in the electronic space of both individuals and states or international organizations. It is concluded that "international digital law" is the same reality as the transnational electronic space regulated by it, only law, as it often happens, lags behind the needs of regulation. International digital law is still an emerging branch of international law.

Keywords: Digital law, International digital law, International law, Domestic (national) law, Branch of international law, International system, Transformation of the international system

Термин «международное цифровое право» в российской международно-правовой литературе и в официальных нормативных актах пока не встречается. Нет его и в международных договорах, в актах международных организаций, в научных работах зарубежных юристов-международников.

В то же время термин «цифровое право» применительно к внутренним системам права разных государств фигурирует довольно часто. При этом российскими и зарубежными авторами используется как сам этот термин, так и заменяющие его или близкие к нему понятия: «компьютерное право», «киберправо», «электронное право», «интернет-право», «информационное право», «сетевое право» и др. [2. С. 110–111]. В правовых науках государств идут научные споры о том, сложились ли уже в национальном праве соответствующие отрасли права и законодательства, могут ли они появиться в принципе и как они могли бы называться.

У этих понятий есть общие черты: все они отражают явление электронного пространства и деятельности в нем при посредстве специальных технологий. Речь идет о некоем искусственном – транснациональном – пространстве, созданном человеком, и действуют в нем (взаимодействуют или противостоят друг другу) как частные лица, так и государства, международные организации.

Важно, что к созданию и развитию электронной сферы во всей ее полноте и сложности причастны транснациональные корпорации, прежде всего, США и других технологичных стран. Другими словами, цифровое пространство – это некая транснациональная среда, которая создана и живет преимущественно по правилам, определяемым частными субъектами-операторами. При этом цифровые технологии вполне могут быть использованы как «оружие», как средство «агрессии».

Вокруг управления глобальным Интернетом идет борьба государственных интересов. Под давлением незападных государств инфраструктура управления Интернетом понемногу видоизменяется: в США в свое время была создана Корпорация по присвоению имен и адресов в Интернете (ICANN); какие-то мероприятия проводятся под эгидой ООН (Всемирная встреча по вопросам информационного общества в 2003–2005 гг., с принятием Декларации и Принципов). Противоречие между частным и глобальным статусом интернет-пространства и интересами большинства государств, включая Россию, налицо. Россия выступает за то, чтобы стандарты управления Интернетом разрабатывались и внедрялись на базе Международного союза электросвязи, но пока проблема не решается.

Быстрорастущие электронные пространства и компьютерные сети в государствах, усложнение и конфликтность отношений, связанных с этим, привели к тому, что в национальных правовых системах появились необходимые нормы для регулирования таких отношений – были приняты новые законы или дополнены действующие; стали оформляться целые нормативно-правовые институты.

На примере появления и развития институтов, касающихся развития интернет-технологий (кибертехнологий, информационных или сетевых технологий –

названия часто разнятся), прослеживается закономерность, характерная для всего международного права и/или отдельных его институтов и отраслей. Закономерность заключается в том, что сначала новые, усложняющиеся отношения регулируются внутри соответствующих государств посредством национальных правовых актов, потом происходит *интернационализация* новых отношений и связанных с ними проблем – и государства вынуждены договариваться о том, как регулировать подобные отношения за пределами национальных границ, как сообща решать возникающие проблемы, а для этого заключают необходимые международные договоры или формируют международные обычаи. Именно эти процессы наблюдаются в настоящее время в цифровой сфере.

В первую очередь под правовое регулирование внутри государств попали наиболее сложные и важные для власти и общества отношения: цифровые права человека; проблематика связи и информационная безопасность; защита потребителя в цифровой сфере услуг; вопросы интеллектуальной собственности, электронные договоры и электронные подписи, интернет-платежи и налоговая сфера – все они нашли отражение в специальных законах, в гражданском, уголовном, административном и иных отраслях законодательства [5. С. 3–13]. К этому предмету регулирования сегодня добавились или добавляются: интернет вещей, искусственный интеллект, криптовалюты. Цифровая сфера охватывает всю повседневную жизнь: спорт, здравоохранение, образование, транспорт, торговлю, прочие сектора экономики и т. п. Формирующиеся или уже созданные цифровые институты права по факту обслуживают многие другие – традиционные – отрасли внутреннего права.

Разнородное национальное законодательство и разброс государственных интересов у разных стран объективно породили необходимость в международно-правовом регулировании тех аспектов деятельности в электронном пространстве, по которым можно договориться. На наших глазах родились и рождаются многосторонние международные договоры. Следует обратить внимание, что большинство нормативных актов по регулированию цифровой среды инициируется в рамках законодательства США и других западных стран; затем часть вопросов выносится этими странами в международные договоры или в мягкое право [4. С. 9–20]. Мягкое право дает толчок для смены метода регулирования – перевода его на международно-правовой уровень.

Кардинальный вопрос, потребовавший ясности: как электронное пространство, порожденное и развивающееся под эгидой транснациональных корпораций, с его «свободой», совмещается с принципом государственного суверенитета. Информационные корпорации выступали за максимальную свободу Интернета, против любого вмешательства государства, однако государства в конце концов приступили к регулированию данного транснационального пространства и контролю за ним.

Одним из важнейших принципов стал закрепленный сначала во внутреннем праве, а потом в международных актах принцип цифрового суверенитета государства. В силу этого принципа, например, Россия на законодательном уровне формирует свою юрисдикцию в электронной сфере и в ее рамках, в частности, требует хранить цифровые персональные данные на территории России, натыкаясь на противодействие господствующих информационных корпораций.

На примере защиты персональных данных хорошо прослеживается закономерность становления национальных и международно-правовых институтов в электронной сфере в целом в контексте цифрового суверенитета. Первые национальные законы в этой сфере стали появляться в 80-х гг. XX в. В ряде случаев данная проблематика переместилась в органы международных организаций регионального уровня, например в Совет Европы; в его рамках в 1981 г. была подписана Конвенция № 108 о защите персональных данных физических лиц (Россия присоединилась в 2001 г.). На основе концептуальных положений Конвенции в России был принят Закон «О персональных данных» (2006). Таким образом, международный нормативный акт выступил инструментом рецепции правовых норм и унификации национального законодательства.

Проблема унификации внутреннего права в цифровом пространстве по-прежнему остается острой. Даже в рамках Евразийского экономического союза (ЕАЭС) действуют свои правила, касающиеся защиты персональных данных: национальное законодательство государств – членов ЕАЭС разобщено, не унифицировано.

Из огромного набора вопросов, касающихся цифровой сферы и находящихся под регулированием средствами национального законодательства, лишь малая часть передана под международно-правовое регулирование. Многосторонние международные договоры, на регулирование которых вынесена цифровая проблематика, сравнительно немногочисленны. Сюда можно добавить «старые» универсальные договоры, касающиеся радиовещания, телевидения, связи, компьютерной информации и т. п. [3].

Следует учесть и общепринятые принципы международного права: они также задействованы в регулирование отношений в международной информационной системе – в глобальном информационном обществе [1. С. 261–268].

Определенная компетенция относительно вопросов цифровой проблематики имеется у некоторых – многих – международных организаций: ООН, ЮНЕСКО, ВОИС, ВТО, ЮНСИТРАЛ, ОБСЕ, ОЭСР и др. В рамках ВОИС, например, осуществляется управление двумя десятками соглашений, связанных с авторским и патентным правом, статусом фонограмм, компьютерных программ и т. д. В рамках ЕС принимаются соответствующие директивы: Директива ЕС 2018/1673 о борьбе с отмыванием денег и т. п. Борьбой с использованием в преступных целях цифровых технологий на международном уровне озабочены и разнообразные параорганизации: Группа-7, БРИКС и другие, – принимающие рекомендательные и декларативные акты. Группа-7, например, приняла Декларацию об ответственном поведении государств в киберпространстве (2017); на совещании министров иностранных дел Г-7 было принято «Динарское заявление об инициативе за нормы в киберпространстве» (2019). Многие акты, касающиеся цифровой сферы, принимаются на разного рода частных конференциях: так, известные и авторитетные «Азиломарские принципы» были приняты в США на международной конференции разработчиков программ искусственного интеллекта (2017). Подобного рода акты не являются правовыми, но оказывают постепенное воздействие на международное правосознание, благодаря которому впоследствии формулируются и продвигаются нормы национального или международного права.

В рамках Комиссии ООН по праву международной торговли – ЮНСИТРАЛ – приняты Типовые законы: об электронной торговле (1996); об электронных подписях (2001). В рамках СНГ принят «Модельный закон об основах регулирования Интернета» (2011). Эти факты показывают пример еще одного правового инструмента регулирования цифровой среды: через разработанные типовые законы для внутренних правовых систем государств происходит постепенная унификация национальных законодательств в том или ином вопросе.

Какая-то часть международных договоров заключена на региональном уровне (в том числе в привязке к отдельным интеграционным объединениям и международным организациям). Обзор таких договоров показывает, что инструментарий международного права пока задействован несущественно и значительно отстает от реальных проблем, разрешение которых назрело [6. С. 1–5]. Государства просто не в состоянии договориться по многим проблемам.

По этой причине ряд других интернационализированных аспектов существования электронного пространства регулируется не международными договорами, а актами мягкого права, и таких актов – великое множество. На универсальном уровне, в рамках ООН, регулярно принимаются резолюции Генеральной Ассамблеи. ЮНЕСКО приняла Хартию о сохранении цифрового наследия (2003): цифровое наследие рассматривается как «общее наследие человечества». Акты неправового, но нормативного характера регулярно принимаются разного рода неправительственными организациями и предпринимательскими ассоциациями.

Итак, под предметом/объектом «международного цифрового права» в широком смысле можно понимать деятельность субъектов международного права – государств, международных организаций – в электронном пространстве и регулируемое ими содержание этого пространства.

С одной стороны, «международное цифровое право» вполне можно считать на перспективу отраслью международного права; очевидны общественная значимость, интерес государств, предметное единство для регулирования; качественное своеобразие нормативного блока, его целостность и практическая значимость. Выделение такой отрасли в системе международного права отвечает интересам сообщества государств. Имеющиеся на этот счет нормы и принципы вполне согласованы между собой, существуют, действуют и развиваются системно; некоторые из них приобрели или приобретают качество jus cogens и erga omnes. При этом формирующаяся отрасль включает в себя ряд международно-правовых институтов, некоторые из них носят комплексный характер.

С другой стороны, на сегодняшний день данный нормативный блок не вполне удовлетворяет некоторым критериям, необходимым для выделения в системе международного права полноценной отрасли. Если объект регулирования посредством «международного цифрового права» в реальности так или иначе потенциально просматривается (это отношения между государствами и/или международными организациями в транснациональном электронном пространстве), то набор фактически регулируемых отношений достаточно узок; нет необходимой содержательной полноты; недостает источников международного права.

В термине «международное цифровое право» слово «цифровое» является наиболее объемлющим, всеохватным применительно к описываемой сфере отно-

шений и понятным, удобным на практике. Термин «международное информационное право» (или аналогичные) представляется недостаточным по предметному наполнению.

Нормы и принципы международного цифрового права сосредоточены пока на нескольких наиболее актуальных вопросах: права человека в электронной среде; управление глобальным интернетом; цифровой суверенитет государства со всеми вытекающими из этого аспектами; цифровая безопасность; сотрудничество государств в разрешении проблем, унификации национальных законодательств и в международно-правовом регулировании деятельности частных субъектов и самих государств (международных организаций) в транснациональном цифровом пространстве – применительно ко всем сторонам жизни человека и общества. Наиболее острой проблемой является, судя по принимаемым международным актам, борьба с международной киберпреступностью.

Следует также видеть, что основным регулятором глобального цифрового пространства остаются нормы, которые созданы интернет-корпорациями и подобными структурами, – нормы, составляющие *транснациональное право*. Данный инструментарий поддерживается со стороны внутреннего права США, западных стран и соответствующих организаций, в том числе актами мягкого права. Транснациональное цифровое право предполагает, что Интернет должен оставаться максимально свободным и анонимным, а контроль государств за ним – минимальным (Декларация Совета Европы 2003 г. о свободе обмена информацией в Интернете). Понятно, что подобный статус цифрового пространства ведет к злоупотреблениям, управляемому использованию Интернета во вред отдельным государствам, для вмешательства во внутренние дела и часто к настоящей информационной агрессии. Все это встречает противодействие со стороны суверенных государств: они внедряют системы лицензирования, блокирования интернет-сайтов и т. п.; принимают необходимые законы и заключают многосторонние и двусторонние международные договоры. В целом роль государственного регулирования в цифровой среде – средствами внутреннего и международного права – увеличивается. Общественное сознание и международное правосознание поддерживают эту тенденцию.

Вместе с тем развитие международного цифрового права вступает в новый этап – одновременно со всей международной системой и системой международного права в целом. В 2014–2022 гг. произошла коренная перестройка мироустройства: миропорядок окончательно разделился как минимум на две части – Запад и «не-Запад» – и стал постепенно превращаться в многополярный. В условиях нарастающей экзистенциальной угрозы существованию России Президент В. В. Путин в феврале 2022 г. отдал приказ о проведении Специальной военной операции по демилитаризации и денацификации Украины, превращенной западными странами в антироссийский военно-политический центр – «Анти-Россию». Позднее президент констатировал: формирование многополярного мироустройства началось. Это означает, что в прежнем виде глобальная международная система не останется; глобализация и пути ее продвижения меняются. Наряду с реалиями международных отношений меняются и надстроечные явления: правовые системы государств, вся система международного права.

Будущий миропорядок будет представлять собой конгломерат двух или более геополитических полюсов силы, опирающихся на «свои» цивилизационные ценно-

сти и интеграционные объединения. Одним из «полюсов» останется Запад; другим автономным цивилизационным пространством является Россия с дружественными странами. На самостоятельную роль «полюса» в сообществе цивилизаций претендуют Китай и некоторые другие крупные государства. Каждый формирующийся (и сформированный) «полюс» будет укреплять отношения внутри него с точки зрения как институциональной, так и нормативной составляющих. Фрагментация системы международного права усилится; соответствующие группы государств будут создавать международно-правовые институты, которые будут учитывать их цивилизационные особенности и геостратегические интересы. Равным образом это будет отражаться в развитии нормативных блоков, касающихся международно-правового регулирования цифрового пространства. Вместе с тем нормы и принципы международного цифрового права, которые уже существуют и имеют универсальный характер, останутся в качестве фундаментальной базы всей растущей отрасли; они будут связывать различающиеся нормативные блоки разных полюсов в нечто общее – в международное цифровое право (уже с другой его системой).

Помимо норм и принципов международного права, в регулировании глобальной цифровой среды, как показано выше, участвуют: транснациональное право, национальное право, мягкое право, нормы международной морали, международное правосознание. В новых условиях роль каждого фактора изменится – по крайней мере в незападном полюсе (или полюсах). Зона транснационального права будет сокращаться. Воздействие национального права и международно-правового инструментария будет возрастать. При этом многосторонние международные договоры во все большей степени будут нацелены на унификацию национальных законов – с особенностями, присущими каждому полюсу. Отставание международного права от реалий международных цифровых отношений будет сохраняться, и это объективное обстоятельство.

В качестве вывода из всего изложенного можно заключить, что международное цифровое право как отрасль международного права еще только формируется, но оно, безусловно, займет свое место в системе других отраслей.

Список литературы

1. Данельян А. А. Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 261–268.

2. Мажорина М. В. Цифровые платформы и международное частное право, или Есть ли будущее у киберправа? // Lex russica. 2019. № 2 (147). С. 107–120.

3. Насер А. А. Международное информационное право. 2020. URL: https://be5.biz/pravo/m026/20.html (дата обращения: 02.09.2022).

4. Печегин Д. А. Правовые механизмы защиты цифрового суверенитета государства: сравнительно-правовой аспект. // Российский журнал правовых исследований. ИЗиСП. 2022. Т. 9, № 2. С. 9–20.

5. Рожкова М. А. Является ли цифровой право отраслью права и нужно ли ожидать появления Цифрового кодекса? // Хозяйство и право. 2020. № 4. С. 3–13.

6. Abid A. Adonis. International Law on Cyber Security in the Age of Digital Sovereignty // E-International Relations. 2020. Pp. 1–5.

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ЧАСТНОПРАВОВЫХ (ЦИВИЛИСТИЧЕСКИХ) ОТНОШЕНИЙ

Е. Н. Абрамова,
кандидат юридических наук, доцент,
Санкт-Петербургский государственный экономический университет

ОСНОВАНИЯ ВОЗНИКНОВЕНИЯ ГРАЖДАНСКИХ ПРАВ НА ЦИФРОВОЕ ИМУЩЕСТВО

Аннотация. Целью исследования является выявление способов возникновения субъективных гражданских прав на цифровые объекты, относящиеся к имуществу: криптовалюту и цифровые права, в том числе цифровые финансовые активы и утилитарные цифровые права. Проводится аналогия между способами возникновения прав на цифровое имущество и способами возникновения вещных прав. Выявляются проблемы, связанные с нарушением основных цивилистических принципов возникновения прав в сложившейся практике операторов информационных систем, которые предлагается преодолеть путем устранения существующих пробелов гражданского законодательства и распространения норм гражданского права на отношения с цифровым имуществом.

Ключевые слова: право, цифровые технологии, цифровое имущество, криптовалюта, цифровое право, цифровой объект, возникновение прав, право собственности

BASIS FOR OCCURRENCE OF RIGHTS TO DIGITAL PROPERTY

Abstract. The purpose of article is to identify ways of the emergence of subjective civil rights to digital objects: cryptocurrency, digital rights, including digital financial assets and utilitarian digital rights. An analogy is drawn between the ways in which rights arise to digital property and real property. The problems associated with the violation of the basic civilistic principles in the established practice of information system operators are identified. It is nessesary to eliminate existing gaps in civil legislation and extende the norms of civil law to digital property.

Keywords: Law, Digital technologies, Digital property, Cryptocurrency, Token, Digital object, Emergence of rights, Property right

Введение. В условиях цифровой трансформации общественных отношений социально-гуманитарные науки не всегда успевают за техническим прогрессом, в результате чего возникает множество пробелов в научном знании и дискурсов по спорным и неоднозначным вопросам. К таким проблемным вопросам в сфере цивилистики относится в числе прочего проблема выявления понятия и установления правового режима цифрового имущества, поскольку, как отмечается в белорус-

ской юридической литературе, «отношения, складывающиеся в ходе разработки и использования цифровых технологий, а также объектов, созданных с их помощью, как правило, носят имущественный характер» [4. С. 29]. По своей сути оно представляет собой информацию в цифровом виде (зашифрованную с помощью двоичного кода), в результате чего в юридической литературе распространился подход к ее правовой квалификации в качестве информации, с чем не представляется возможным согласиться, поскольку информация сама по себе, не облеченная в формат конкретного объекта права, не может выступать объектом гражданского оборота. Информация сама по себе (как сведения, устные и письменные) может быть только доказательством существования объекта, но не им самим.

Для правильного понимания правовой природы цифрового имущества необходимым представляется применение широко распространенного в цивилистике метода юридической фикции, позволяющего распространить на некую (чаще всего новую) сущность правовой режим совершенно другого (хорошо известного) явления. Поэтому неважно, чем фактически является объект, важно, как к нему относится законодатель и право. Другими методами, использованными в проведенном исследовании, стали методы комплексного и системного анализа, сравнения и аналогии.

Целью исследования является обоснование имущественной природы цифрового имущества и допустимость распространения на него существующих гражданско-правовых правил о возникновении прав на имущество.

Основная часть. Прежде всего, следует отметить, что категория «имущество» однозначно не определена в гражданском праве. В ст. 128 ГК РФ оно разделено на две разные сущности – вещи и иное имущество по критерию материальности. В целом имуществом принято именовать такой объект гражданских прав, который имеет имущественно-стоимостное выражение. В этом смысле не любой цифровой объект, т. е. объект, информация о котором существует в информационной системе (цифровой среде), является имуществом.

Из признанных в российском законодательстве цифровых объектов к цифровому имуществу, таким образом, можно отнести цифровую валюту, цифровой рубль и цифровые права. В ст. 128 ГК РФ прямо поименованы только последние, причем отнесены они именно к «иному имуществу», к такой его разновидности, как «имущественные права». В этом качестве цифровые права представляют собой права требования или комплекс прав требования в сочетании с другими правами (например, вещными, неимущественными и корпоративными). Основанием возникновения таких прав выступает определенный юридический факт, в результате которого они возникают у одного из субъектов, а у другого субъекта появляются корреспондирующие таким правам обязанности. При этом выполнение последних заключается в активном поведении, т. е. интерес управомоченного по цифровому праву удовлетворяется осуществлением действий обязанным лицом. По сути дела, речь идет о возникновении обязательства, отличительной чертой которого является лишь то, что запись о его существовании производится в цифровом виде (в информационной системе с помощью системы двойного кодирования). Теоретически возможно распространить на основания возникновения цифровых

прав те же самые основания, которые предусмотрены законом для возникновения обязательства с тем лишь исключением, что в отличие от любых иных обязательств первоначально они возникают только в информационной системе. Данная особенность, как представляется, характеризует такой элемент порождающей обязательство сделки, как форма, т. е. существование в цифровой среде не является сутью, содержанием, а представляет собой прямое волеизъявление, письменное, но с дополнительным требованием – оформления в информационной системе.

Таким образом, основанием возникновения нового цифрового права может быть только договор, заключенный в информационной системе. В дальнейшем это цифровое право может быть передано, как и любое иное имущество, по любым основаниям, предусмотренным гражданским законодательством – по наследству, по решению суда и т. д. Но такой переход необходимо также фиксировать в информационной системе в будущем для возможности осуществления и дальнейшей передачи такого цифрового права.

Особым основанием при этом выступает договор, являющийся основанием возникновения цифрового права. Исходя из общедозволительного принципа правового регулирования, являющегося приоритетным в гражданском праве, можно было бы сделать вывод о том, что по поводу цифрового права может быть заключен любой договор, как в информационной системе, так и вне ее, традиционными способами. Прямого запрета о заключении договора вне информационной системы специальные законы об отдельных видах цифровых прав не содержат. Однако общий смысл и посыл таких законов говорят о специфичности цифрового права и особых требований со стороны регулятора к механизму заключения сделок с ними. Так, в соответствии с п. 1 ст. 10 ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ» (далее – ФЗ о ЦФА) [1] все сделки с ЦФА совершаются через особого субъекта – оператора обмена, к которому и к деятельности которого закон предъявляет особые требования. А согласно п. 7 ст. 8 ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ о привлечении инвестиций) [2], утилитарное цифровое право возникает, обременяется и переходит от одного лица к другому только в инвестиционной платформе. Таким образом, действующее регулирование не признает законными договоры о цифровых правах, заключенные традиционными способами, вне информационной системы. Если признавать такой договор сделкой, заключенной с нарушением требований закона, может возникнуть неопределенность в определении правовых последствий такой сделки. По общему правилу такой договор, согласно ст. 168 ГК РФ, является оспоримым, поскольку маловероятно, что его заключение посягает на публичные интересы или права и интересы третьих лиц. Однако его способность в действительности порождать права и обязанности остается сомнительной даже в отсутствие оспаривания, поскольку запись о цифровом праве, сделанная в информационной системе, останется в силе и не сможет быть изменена на основании такого договора. Поэтому более подходящей представляется такая квалификация оснований недействительного договора, заключенного вне информа-

ционной системы, как нарушение формы сделки, влекущее недействительность в силу прямого указания закона. Такое основание прямо предусмотрено в абз. 4 п. 1 ст. 160 ГК РФ, согласно которому законом могут устанавливаться дополнительные требования к простой письменной форме сделки. Цифровой вид письменной формы, как представляется, и есть такое дополнительное требование к форме сделок с цифровыми правами. Как отмечается в юридической литературе, «объекты цифрового гражданского оборота подлежат … учету и удостоверению в цифровых реестрах посредством цифровых записей компьютерных кодов для подтверждения наличия такого цифрового объекта и его правового статуса» [5. С. 344], отсутствие таких цифровых записей является нарушением формальной стороны обязательства.

Однако для ничтожности договоров с его нарушением необходимо прямое указание об этом в законе. Одного указания на невозможность заключения договора вне информационной системы недостаточно, поскольку в таком случае возникают общие последствия несоблюдения простой письменной формы – запрет ссылаться на показания свидетелей в случае спора (п. 1 ст. 162 ГК РФ). Таким образом, в настоящее время законодательство о цифровых правах, не содержащее нормы о последствиях несоблюдения цифровой формы договора, не позволяет однозначно сделать вывод о недействительности в форме ничтожности договора о переходе или обременении цифрового права. Если суд признает такой договор действительным или существующим, оператор информационной системы обязан внести соответствующие изменения на основании решения суда. Однако существование и эффективность механизма внесения таких изменений в информационную систему требует отдельного исследования в связи с рядом возникающих в связи с этим вопросов. Следует отметить, что и в целом возможность внесения изменений в информационную систему при возникновении цифровых прав вне ее, например в результате правопреемства, на практике остается труднореализуемой в связи с пробелом действующего законодательства.

При этом следует учитывать, что основания возникновения прав на цифровые права не совпадают полностью с основаниями возникновения обязательства. Несмотря на то, что цифровые права квалифицируются в российском законодательстве как имущественные права, не являющиеся вещами, подобное отношение к ним не является единственно возможным. Так, согласно п. 3 Приложения 1 к Декрету Президента Республики Беларусь № 8 [3], цифровой знак (токен) отнесен к объектам вещных прав. Это означает, что возникновение прав на цифровое имущество осуществляется аналогично возникновению вещных прав. Способы приобретения права на токены, криптовалюту, как централизованную, так и нецентрализованную, совпадают со способами приобретения вещных прав, т. е. могут быть первоначальными и производными.

К первоначальным относятся такие способы, с помощью которых право приобретается впервые, а до этого право на данный объект ни у кого не существовало. К таким способам можно отнести создание криптовалюты майнером. По сформированному деловому обыкновению майнер приобретает право собственности на криптовалюту, созданную им по правилам информационной системы, выпускаю-

щей криптовалюту. Кроме того, майнер может получать криптовалюту в качестве вознаграждения за обработку информации о цифровой операции. Иное может быть предусмотрено правилами информационной системы или договором между майнером и заказчиком, поскольку майнер может действовать в интересах такого третьего лица, осуществляя майнинг по его заказу.

Несмотря на распространенную в технократической и экономической среде терминологию, с правовой точки зрения такое «создание» не является «созданием вещи», как оно представлено в цивилистике, а выступает встречным предоставлением за выполнение работы по вычислению нонса (поддержанию функционирования информационной системы). Однако вычисленный нонс завершает сделку между конкретными субъектами, т. е. передает права на криптовалюту от одного из них к другому. По правилам информационной системы это влечет появление определенного количества криптовалюты у майнера. Такой способ возникновения права является первоначальным, поскольку ранее на эту цифровую валюту прав ни у кого не было.

Поскольку майнер поддерживает работоспособность системы, его деятельность вознаграждается по правилам информационной системы. Такое вознаграждение, как правило, осуществляется в той криптовалюте, сделки с которой он обрабатывает. Вознаграждение майнер может получать как от информационной системы, так и от пользователя, который сам назначает его размер как вознаграждение за совершение транзакции. Свобода пользователя, совершившего сделку с криптовалютой, в определении размера вознаграждения майнера ограничивается лишь временем ожидания, которое для него допустимо. Так, незначительный размер оплаты услуг майнера может привести к долгому неподтверждению сделки майнером, который предпочтет завершить сделки, по которым обещано высокое вознаграждение. Представляется, что первоначальным способом возникновения права на криптовалюту является получение майнером цифровой валюты только от информационной системы, поскольку сам оператор информационной системы не имеет прав на предоставляемую валюту. Однако криптовалюта, получаемая майнером как вознаграждение от пользователя, как представляется, является натуральной формой оплаты услуг майнера, поэтому у последнего права на такую криптовалюту возникают по производному способу – на основании договора между ним и пользователем, поскольку пользователь может предложить контрагенту только ту криптовалюту, права на которую у него есть или будут.

Самое значительное вознаграждение от информационной системы майнер получает в начале выпуска новой криптовалюты, по мере завершения определенного правилами информационной системы количества сделок вознаграждение майнера уменьшается. Так, первоначальное вознаграждение майнера за майнинг биткоина составляло 50 биткоинов. Каждые 210 тыс. сделок (блоков) вознаграждение уменьшается в два раза, и на данный момент майнер получает около 10–20 биткоинов. Когда будет выпущен установленный правилами информационной системы максимум по количеству данной криптовалюты, новая криптовалюта данного вида выпускаться уже не будет. Так, может быть выпущено не более 21 млн биткоинов, в данный момент уже выпущено почти 18 млн. Но и при достижении указанного максимума, как

предполагают специалисты, работа информационной системы будет продолжена, поскольку сделки с биткоинами будут заключаться и после его достижения.

Для централизованной криптовалюты и токена майнинг не характерен, поэтому путем «создания» право, например на цифровой рубль, не возникает. Однако первоначальным способом приобретения права на любое цифровое имущество можно считать его приобретение в результате «первичного выпуска». Как и в случае с ценной бумагой, первоначальные права на которую получает первый приобретатель, получивший ее от должника, выпустившего ее, криптовалюту можно получить впервые, от выпустившего ее оператора. Несмотря на то, что основанием возникновения в этом случае является договор, криптовалюта не переходит при этом от одного лица к другому, а возникает впервые именно у первого приобретателя. До появления криптовалюты в обладании первого приобретателя она не существует.

Иные первоначальные способы приобретения права на цифровое имущество пока не получили распространения, хотя теоретически можно представить получение криптовалюты или цифрового права в результате находки, клада, приобретения прав на бесхозяйную криптовалюту и т. п. Например, правила некоторых информационных систем предусматривают приобретение прав на криптовалюту, обладатель которых прекратил деятельность в информационной системе. Учитывая, что идентификация пользователя может не позволять определить субъекта права, создавшего идентификационную запись и приобретавшего криптовалюту, оставшуюся на его цифровом кошельке, цифровую валюту можно квалифицировать как бесхозяйную. Такую криптовалюту, как правило, информационные системы считают своей при соблюдении указанных в ее правилах условий. Представляется, что правила о возникновении прав на криптовалюту должны быть сформированы законодателем, а не правилами информационной системы, которые подчас не соблюдают требований национальных законодательств и нарушают права пользователей. Также возможна ситуация, при которой пароль доступа (приватный ключ и т. п.) к электронному кошельку найден или обнаружен третьим субъектом. Такой способ может быть квалифицирован как находка, клад или отказ собственника от права на цифровой объект. В настоящее время такие ситуации считаются неурегулированными законодательством, поскольку специальные законы о цифровом имуществе не содержат соответствующих правил. Однако подобный вывод не может считаться обоснованным. Для любого имущества должны действовать общие правила оборота, в том числе о возникновении прав на него, независимо от способа существования информации о правах и объектах. Поэтому в указанных выше случаях должны применяться общие правила ГК РФ о возникновении права собственности. При этом правила информационных систем не могут содержать правила, противоречащие действующему законодательству, что сегодня, к сожалению, повсеместно распространено. Иной подход создает возможность для недобросовестного поведения и злоупотреблений правом со стороны оператора информационной системы.

Основным производным способом приобретения права на криптовалюту является переход прав на нее по сделкам.

Самой распространенной сделкой, по которой можно приобрести цифровую валюту, является договор. При этом следует отличать договоры, в которых криптовалюта выступает средством платежа, от договоров, по которым она является предметом договора.

Первую разновидность договоров российское законодательство не поддерживает. Во-первых, цифровая валюта не признается законным средством платежа, т. е. она не имеет принудительной силы, не обязательна к приему. Во-вторых, действующее российское законодательство отрицательно относится к сделкам, субъекты которых согласились принять к приему криптовалюту в качестве встречного предоставления. Так, согласно п. 5 ст. 14 ФЗ о ЦФА, российские субъекты, а также находящиеся в течение определенного времени на территории РФ иностранные лица не вправе принимать цифровую валюту в качестве встречного предоставления за передаваемые ими товары, выполняемые работы, оказываемые услуги или иного способа, позволяющего предполагать оплату цифровой валютой. Последствием нарушения такого запрета является отказ в предоставлении судебной защиты прав, связанных с обладанием криптовалютой (п. 6 ст. 14 ФЗ о ЦФА). Исключением из названного общего правила является предоставление судебной защиты при условии информирования о фактах обладания цифровой валютой и совершения гражданско-правовых сделок в порядке, установленном налоговым законодательством, т. е. при условии оплаты предусмотренных НК РФ налогов для данных видов сделок и операций и своевременного направления уведомлений, форма которых пока не определена.

Вторая разновидность договоров, по которым криптовалюта выступает объектом, российским законодательством разрешена, хотя и не урегулирована должным образом. Прежде всего, как отмечалось выше, отсутствует ясное представление о возможности и последствиях договоров, заключенных вне информационной системы, отсутствует механизм выявления результатов технических сбоев и иных ошибок и т. п.

Как представляется, не исключены для криптовалюты и другие производные способы приобретения прав на нее, например, приватизация, конфискация, реквизиция, наследование, реорганизация и др. Однако никакого правового механизма учета таких фактически возникших прав действующее российское законодательство не предусматривает. Для этого необходима разработка перечня оснований для внесения в информационную систему соответствующих изменений. Помимо этого, важным представляется признать распространение на криптовалюту норм гражданского законодательства как общего правила в целях избежания злоупотребления правами сильной стороной договора (оператора информационной системы), обхода закона третьими лицами и других правонарушений. В условиях пробела специального законодательства о цифровых правах возникает иллюзия неурегулированности таких отношений и возможности заполнения таких пробелов правилами информационных систем, что не может считаться правомерным. Так, правилами некоторых информационных систем предусматривается передача в собственность оператора криптовалюты умершего пользователя, даже если его наследники знают о наличии криптовалюты и могут доказать свои права.

Таким образом, налицо необходимость признания цифрового имущества имуществом в гражданско-правовом смысле. Подобный подход будет способствовать более гармоничному развитию специального законодательства, которое пока развивается больше в техническом, чем цивилистическом русле, защите прав обладателей цифрового имущества и его правопреемников.

Заключение. Исследование способов возникновения прав на цифровое имущество выявило следующие закономерности.

Во-первых, существуют две группы способов возникновения прав на цифровое имущество. К первой группе можно отнести способы возникновения обязательства, на основании которых возникают права на такое цифровое имущество, как цифровое право. Являясь по своей правовой природе имущественным правом, т. е. иным имуществом, по формулировке ГК РФ, цифровое право возникает теми же способами, что и любое право (требование). К другой группе оснований можно отнести способы возникновения вещных прав, на основании которых возникают права на любое цифровое имущество в результате применения к нему приема юридической фикции, благодаря чему обязательство и его форма считаются объектом гражданских прав в целях удобства гражданского оборота.

Во-вторых, применимость вещно-правовых способов возникновения прав на цифровое имущество позволяет установить его место в системе объектов гражданских прав. Цифровое имущество можно считать квазивещами, т. е. объектами, не являющимися вещами по своей сущности, но на которые распространяется правовой режим вещи в целях правовой экономии и целесообразности.

В-третьих, цифровизация гражданского оборота, породившая множество новых сущностей, не знавших аналогов, не обязательно должна ломать сложившуюся систему регуляции общественных отношений. Большинство достижений цивилистики легко решают те «проблемы», которые появились в результате исключительно нежелания применения к новым сущностям и конструкциям давно сложившихся и многие века неоднократно справлявшихся с техническим прогрессом и коренной ломкой жизненных устоев правил. Попытки «нарастить» новые правила для новых явлений, игнорируя существующие, только усложнят и запутают правовое регулирование цифровых объектов. Внезапное и стремительно созданное в попытке успеть за идущими невиданными, нарастающими с каждым днем изменениями новое регулирование не может объективно учесть все те нюансы, которые кропотливо и тщательно разрабатывались тысячелетиями. Традиционные правила априори более выверены, системны и эффективны, чем подверженные влиянию технической моде, сшитые на скорую руку, под девизом «все устарело», технонормы.

Список литературы

1. Федеральный закон от 31.07.2020 № 259 «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 13.09.2022).

2. Федеральный закон от 02.08.2019 № 259 «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные зако-

нодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 13.09.2022).

3. Декрет Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 13.09.2022).

4. Гладкая Е. Н. Основные направления развития вещных правоотношений в контексте внедрения цифровых технологий // Актуальные проблемы гражданского права. 2021. № 2 (18). С 27–43.

5. Карцхия А. А. Гражданско-правовая модель регулирования цифровых технологий: дис. … д-ра юрид. наук. Москва, 2019. 394 с.

Р. Н. Адельшин,
кандидат юридических наук, доцент,
Российский государственный университет правосудия

ТЕСТ НА ЛЕГИТИМАЦИЮ СОДЕРЖАНИЯ ЦИФРОВОГО ОБЯЗАТЕЛЬСТВА В КОРПОРАТИВНОМ ИНВЕСТИЦИОННОМ ПРАВЕ

Аннотация. Рассмотрены аспекты частного и публичного характера норм Гражданского кодекса Российской Федерации, вводящих новые объекты гражданских прав: инвестиционные токены акций, производные финансовые инструменты или их аналоги – цифровые права и обязательства. Освещены стохастические смарт-обязательства как особая категория фидуциарных обязательств, цифровых прав как новых объектов гражданских прав на основе договора, а также эффективность применения модели правового регулирования обязательственных правоотношений. Рассмотрены цифровые финансовые активы, специфические корпоративные правоотношения в области «токенизации» активов в виде осуществления прав по производным финансовым инструментам и отказа от права, в том числе по договору между форекс-дилером и физическим лицом, и иные правоотношения, предполагающие осуществление прав с использованием технических и электронных средств.

Ключевые слова: стохастические обязательства, права в распределенном реестре, право на исходный код программы, цифровой финансовый актив, производный финансовый инструмент, права на инвестиционный актив производного финансового инструмента, автоматизированное исполнение обязательства, смарт-контракт, осуществление прав по договору, деривативы, форекс-дилер, автоматизированное исполнение, реализация контрактных прав, заключение договора, расторжение договора

TEST FOR THE LEGITIMATION OF THE CONTENT OF A DIGITAL OBLIGATION IN CORPORATE INVESTMENT LAW

Abstract. The article deals with the provisions of changing the norms of the Civil Code of the Russian Federation in part of new objects of civil rights: investment tokens for shares, digital rights for information technology, derivative financial instruments

or their equivalents, obligations. Stochastic smart-obligations as the special part of fiduciary obligation, the issues of liability regarding digital financial assets, digital rights, as new objects of civil rights on the basis of the contract are touched upon, the effectiveness of the application of the model of legal regulation of legal obligations. This article introduces especially corporate area and will discuss the implementation of rights on derivatives involving a contract with a forex dealer. It will also consider the possibility of applying the institutions of the refusal to execute the contract, the waiver on such contracts and some other legal relations involving the exercise of rights using technical and electronic means. Additionally, the provisions of the Federal Law No. 259 'On digital financial assets' was analyzed.

Keywords: Special fiduciary obligation, Stochastic obligation, Liability for violation of digital rights, Rights in a distributed registry, the Right to the source code of a program, Digital financial assets a derivative financial instrument, Rights to an investment asset. Derivatives, Automated performance, Implementation of contact rights, Unilateral refusal of a contract, Professional participant of the securities market in finance area, Smart contract, Exercise of contractual rights (conclusion of a contract), Derivatives, Forex dealer, Automated performance, Implementation of contact rights, Conclusion of a contract, Termination of a contract, waiver

Введение. Современные перспективы развития гражданского права во многом связаны с правоприменительным аспектом использования цифровых технологий в сфере имущественных отношений и определяются будущим осознанием эффективности применения модели правового регулирования обязательств в сфере цифровых прав и возможностей гражданского оборота цифровых технологий.

Суждение о характеристике в качестве нового объекта гражданского права – «цифровое имущество» – основано на отсутствии вещественной формы, является алгоритмическим кодом, есть результат работы компьютерной программы (в виде компьютерных вычислений), не может использоваться и обращаться вне рамок информационной системы, владелец которой встроен в соответствующую инфраструктуру и стоимость которого для участников этой системы выражена в производной форме. Сам смарт-контракт может различаться, выступать и как компьютерный код, и как правоотношение [4. С. 23–30].

Задачей практического назначения использования прав в распределенном реестре данных и возникающих на основе этого обязательств из цифровых активов для дальнейшего использования в отечественном корпоративном праве для целей инвестирования остается открытым и дискуссионным. Острейшая часть дискуссии на общем запретительном законодательном фоне определяет необходимость в исследовании данных правовых явлений при использовании в качестве инструмента инвестирования токенов акций.

Тест на легитимацию цифрового обязательства для инвестиционных сделок.

Появление в результате реформы первой части ГК РФ в п. 3 ст. 48 Кодекса формулировки о том, что к юридическим лицам, в отношении которых их участники имеют корпоративные права, относятся корпоративные организации, дало смешение понятий о присутствии у обладателей долей (акций) имущественных прав на

имущество юридических лиц и унитарный – корпоративный характер юридического лица, повлекло затруднение квалификации правоотношений относительно «токенизации» прав (использование записей в распределенном реестре данных в информационной системе для целей инвестирования), например на акции и, соответственно, сделок с ними. В законодательстве России нет обобщенного понятия «цифровые активы», которое включало бы «токены, криптовалюту, большие данные, доменные имена и аккаунты, виртуальное игровое имущество и т. д.» [5. С. 19–38].

Кроме того, попытки заменить обязательственные отношения между акционерами и хозяйственным обществом корпоративными отношениями при «токенизации» делают этот подход еще более затруднительным, так как смешивают обязательственные права требования и неимущественные права. Не отвечает на этот вопрос и доктрина корпоративного права в области распорядительных и имущественных сделок.

Существенным и значимым представляется тезис о том, что цифровая валюта – это не право лица, а его имущество в виде электронных данных, но не являющихся цифровыми правами. Тогда как для целей участия в капитале непубличного акционерного общества, в свою очередь, цифровой актив не может быть воспринят за рамками информационной системы, хотя бы и являясь при этом денежным требованием либо правом по ценной бумаге. Очевидно, что служебный токен (олицетворение организационного, неимущественного характера правоотношений) в смысле управления корпоративными организациями имеет юридический смысл в виде особых данных – цифровых «меток». Наряду с этим обязательственные права требования (инвестиционный токен), в отличие от прав, связанных с управлением корпоративными организациями, имеют объект корпоративных отношений имущественного содержания. Такое деление представляется корректным и с точки зрения распорядительных и имущественных сделок в этой сфере.

А в случаях оценки этих положений существует дискуссионное мнение, что абсолютизируются такие два вида новых экономических благ, как цифровые права и права участия в капитале непубличного акционерного общества, которые предстают только в совокупности электронных данных (цифрового кода или обозначения) и которые требуют предварительной деятельности по оказанию услуг в реальном смысле исполнения обязательств (передачи имущества, работ, услуг), направленных на обеспечение выпуска цифровой валюты или выпуска акций в виде цифровых финансовых активов [2. С. 340–345]. К примеру, дефиниции п. 8 ст. 1 Закона о цифровых финансовых активах означают, что без привязки гражданских, а также корпоративных прав к информационной системе цифровые права как объекты гражданских прав возникать и существовать не могут. Пользователи информационной системы являются ее узлами, т. е. частями «цепи», и на основе распределенного реестра данных (как пример – «блокчейн») в последующем как совокупности баз данных обеспечивают верификацию информации с помощью специальных процедур и соответствующих записей.

Однако такой подход в «чистом виде» не характеризует любую информационную систему как «непригодную» к использованию таких прав в распределенном

реестре данных (как «блокчейн» или иная) для структурирования инвестиционных сделок. Более значимым фактором следует назвать отсутствие инфраструктурно-технической готовности для ICO и STO и возможности для появления такой «сделкоспособности», которая даст с учетом взвешенного подхода законодателя к статусу «информационно-технических посредников» ту правовую инфраструктуру, которую в действительности имеют в виду потребители и исполнители с учетом наименьшего ущерба правопорядку. То есть тех оракулов, которые обеспечивают взаимодействие смарт-контракта с внешним информационным источником [3. С. 372–376]. Представляется, что имеющиеся гражданско-правовые договорные конструкции дать ответа на эти вызовы пока не могут, как и равно не дает такого ответа и структура обязательства с участием третьего лица (информационного посредника, агрегатора и др.), в том числе в качестве агента по соответствующему договору.

Только с учетом такой «надстроечной» потенциальной правовой парадигмы – в качестве гипотезы – станет возможным и в дальнейшем совершение таких инвестиционных сделок, в том числе «токенизации» – STO, в локальных информационных системах и, как следствие и как причина, – недостаточность правовой инфраструктуры, в то числе не сформировавшегося «класса посредников» юридических лиц (обладателей информплатформ; технических и технологических посредников) – для уяснения взвешенных правил для сторон обязательств, к примеру передачи и ведения реестра данных, единым регулятором и/или сообществом, стандартизации локальных правил информационных систем и др.

Так, примером использования «токенизированных» цифровых прав могут служить их идентификация и отождествление с цифровыми формами учета, создающими некие «оболочечные» стоимости, пока без конкретизации их содержания.

Таким же образом «генерация» стоимостей на основе определения их в качестве базисного актива в цифровой среде перспективно предполагает, что стоимостные критерии и формы идентификации их в качестве эквивалента финансового участия, например в уставном капитале непубличного акционерного общества, будут корректны и перспективны при условии отражения в соответствующей норме. Таким примером могут служить процедурные вопросы, во-первых, идентификации таких активов в качестве базовых, во-вторых, секьюритизации таких активов в результате предложения и выпуска, совокупности гражданско-правовых сделок, в том числе с эквивалентами, связанными с акционерным капиталом, включая ценные бумаги и получение в результате этого действия корректной стоимости права на актив для последующего использования в таком обязательстве. Основой пока служит только нормативно определенная дефиниция ст. 13 Федерального закона № 259-ФЗ «О цифровых финансовых активах» о выпуске цифрового финансового актива, удостоверяющего право участия в непубличном акционерном обществе. С учетом изложенного инвестиционная функция такой записи в распределенном реестре данных («токене») пока видится призрачной и малоэффективной в российской юрисдикции. Указанное нивелирует смысл такого инвестирования, поскольку обособление прав на «токены», удостоверяющие право на получение прибыли

и право голоса в одном обществе, могут пока существовать только отдельно и сепарированно от акций другого общества, в которые, к примеру, первое собралось инвестировать.

«Токенизированные» активы – распределенные в реестрах данных права – могут быть отнесены к видам имущества при наличии особой стандартизации и при положительном решении о секьюритизации актива, составляющего имущество. Так, и аналогично в последующем, в предмет сделок могут входить имущественные комплексы и обязательства в результате перевода долга. То есть переход обязанностей может связываться с фактом перехода имущественных прав по сделке и включаться в распределенный реестр данных (блокчейн).

Понятийный аппарат категории «цифровой актив» не включает характеристику базового актива, как это сделано государственным регулятором в отношении сделок с производными финансовыми инструментами на централизованной основе, если таковые не являются электронной записью.

Представляется существенным и дискуссионным суждение о том, что «стоимостью обладает не сама запись кода, а удостоверенное ею право на зашифрованный в ней объект, включающее в себя правомочие на доступ к коду (логину, паролю, «криптокошельку» и т. п.), а также правомочие на распоряжение цифровыми активами» [5. С. 34–37].

В связи с этим существенными, но не критичными для будущих возможностей законодателя являются тезисы о возможном выпуске акций в виде цифровых финансовых активов непубличным акционерным обществом, подчеркивающим его виртуальный статус-кво, несмотря на отрицание некоторыми авторами в доктрине [2. С. 17–21]. Одновременно не следует забывать о запретительных положениях, установленных в законодательстве. Кроме того, существует мнение, что правилами отдельно взятой информационной системы некорректно признать возможности совершения сделок с «цифровыми валютами» как с иным имуществом, подчеркивается, что цифровая валюта как в качестве платежа, так и в качестве инвестиции не связана непосредственно с каким-то конкретным обязательством. Цифровая валюта – это совокупность электронных данных, имеющая имущественную ценность в какой-либо информационной системе; она создается в соответствующей информационной системе, и в отношении нее отсутствует обязанное лицо перед каждым носителем – обладателем данных. Исключение составляют операторы системы как особый класс информационных посредников в соответствии с правилами системы, нормативные границы (правила) для деятельности которых пока не установлены.

Заключение. Гражданско-правовой метод при использовании цифровых прав позволяет обосновать концептуальную оценку цифрового гражданского оборота, который в своем содержании предполагает смену носителей цифровых прав посредством применения цифровых технологий, обеспечивающих последовательные математические операции компьютерного кода в виде цифровых записей, служащих формой выражения удостоверения и передачи цифровых гражданских прав на цифровые объекты. То есть смарт-договор реализуется на основе принципа contract formation через программное обеспечение, посредством которого

воля сторон выражается в момент достижения соглашения по условиям договора, а смарт-контракт в виде программного продукта покрывает обычный гражданско-правовой договор.

Тезис о характеристике в качестве нового объекта гражданского права – «цифрового имущества» – основан на отсутствии вещественной формы, поскольку оно есть результат работы компьютерной программы (в виде компьютерных вычислений), а значит, не может использоваться и обращаться вне рамок информационной системы. Однако перспективно возможность существования самой модели «цифрового имущества» в качестве объекта вне информационной системы не исключается. Сам смарт-контракт может различаться как компьютерный код и как правоотношение.

В законодательстве России нет обобщенного понятия «цифровые активы», которое включало бы токены, криптовалюту, большие данные, доменные имена и аккаунты, виртуальное игровое имущество и т. д. В связи с этим пока являются невозможными инвестиционные сделки по поводу «токенизации» акций. Такая норма могла бы быть принята в будущем, когда бы доля в уставном капитале была частью обязательственного права требования (токена) акционера к обществу. И право на токен, будучи частью права требования к обществу, могло бы вовлекаться в оборот как имущество. А так как, согласно ст. 93 ГК РФ, доли в уставном капитале могут разделяться на части, обязательственные отношения из них являются обязательствами с множественностью кредиторов с законодательно возможной реализацией по частям.

Список литературы

1. Андреев В. К. О цифровых правах и «цифровых активах» // Право и бизнес: обеспечение баланса правовых интересов предпринимателей, потребителей и государства: сб. материалов X Междунар. науч.-практ. конф. (Москва, 3 июня 2021). Москва: РГУП, 2022. С. 361–370.

2. Андреев В. К. Правовое и цифровое регулирование предпринимательской деятельности // Журнал предпринимательского и корпоративного права. 2021. № 1. С. 17–21.

3. Белых В. С. Болобонова М. О. Проблемы правового регулирования смарт-контракта в России // Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: моногр. / отв. ред. В. А. Вайпан, М. А. Егорова. Москва: Юстицининформ, 2019. С. 97–116.

4. Ефимова Л. Г., Сиземова О. Б. Правовая природа смарт-контракта // Банковское право. 2019. № 1. С. 23–30.

5. Санникова Л. В., Харитонова Ю. С. Цифровые активы: правовой анализ. Москва: 4 Принт, 2020. С. 304 с.

А. П. Алексеенко,
кандидат юридических наук, доцент,
Санкт-Петербургский государственный университет

РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПЛАТФОРМ ЭЛЕКТРОННОЙ КОММЕРЦИИ: ОПЫТ РОССИИ И КНР

Аннотация. Целью исследования является обзор законодательства КНР и России в сфере регулирования электронной коммерции для определения направлений развития российской правовой базы в данной сфере. В статье рассматривается система нормативных правовых актов России и Китая, касающихся регулирования деятельности платформ электронной коммерции. Выявлено, что в КНР законодатель закрепил нормы, направленные на защиту прав потребителей, внутриплатформенного бизнеса, также предусмотрены правила разрешения споров, возникающих внутри платформы. Кроме того, на уровне провинций и муниципалитетов в Китае осуществляется поддержка развития трансграничной электронной коммерции. Сделан вывод о том, что опыт КНР может быть полезным при создании российского специального закона, регулирующего e-commerce.

Работа выполнена при финансовой поддержке РФФИ проект № 21–511–93004 «Верховенство закона в цифровой экономике Китая и России: современное состояние, проблемы и перспективы».

Ключевые слова: электронная коммерция, агрегатор, оператор платформы, трансграничная торговля, онлайн-торговля, потребители, право КНР

REGULATION OF E-COMMERCE PLATFORMS: RUSSIAN AND CHINESE EXPERIENCE

Abstract. The purpose of the study is to review the legislation of the People's Republic of China and Russia concerning e-commerce and to determine the directions of development of the Russian legal framework in this area. The article examines the system of legal acts of Russia and China regulated e-commerce platforms. It is argued that there are provisions aimed to protect the rights of consumers, intra-platform business in China. Also there are rules for resolving disputes arising within the platforms. Chinese authorities support development of cross-border e-commerce at the provincial and municipal levels. Therefore, it is concluded that the experience of the PRC can be useful in creating a Russian special law on e-commerce.

The reported study was funded by RFBR, project No 21–511–93004 «The rule of law in the digital economy in China and Russia: current state, challenges and future development».

Keywords: E-commerce, Aggregator, Platform operator, Cross-border trade, Online commerce, Consumers, Chinese law

Введение. Сфера электронной коммерции является одним из наиболее перспективных и быстроразвивающихся направлений предпринимательской деятельности в большинстве государств [20]. Российская Федерация не является

исключением. Согласно данным Единой межведомственной информационно-статистической системы, в декабре 2021 г. в России доля продаж через Интернет в общем объеме оборота розничной торговли составила 4,8 % [6]. Данный показатель вырос на 23 % по сравнению со значением декабря 2020 г. Однако в России до сих пор нет специального закона, посвященного урегулированию деятельности платформ электронной коммерции и внутриплатформенного бизнеса, что порождает множество вопросов [18], в том числе касающихся ответственности агрегатора (платформы) перед потребителем товара или услуги [14] и разрешения возникающих в этой связи споров [15].

КНР является одним из мировых лидеров сферы e-commerce. Согласно данным статистики, в 2021 г. на Китай пришлось более половины мировых розничных продаж электронной коммерции. Доля цифровой экономики составила 39,8 % от ВВП данной страны, а объем оборота электронной коммерции равнялся 7,1 трлн долларов США [19]. Китай развивает электронную коммерцию не только внутри страны, но и продвигает трансграничную торговлю. Китайские платформы, принадлежащие компаниям Alibaba, JD.com, Pinduoduo, прочно занимают место в международном товарообмене.

КНР имеет разветвленную базу специальных нормативных правовых актов, направленных на урегулирование сферы e-commerce [16]. Данный факт обуславливает важность изучения опыта Китая в целях формирования отечественного законодательства об электронной коммерции. Это, с одной стороны, помогло бы дать дополнительный импульс развитию цифровой экономики, а с другой – создало бы необходимые правовые гарантии для потребителей и внутриплатформенного бизнеса.

Законодательство КНР об электронной коммерции. Регулирование электронной коммерции в Китае осуществляется на национальном, провинциальном и местном уровнях. На общекитайском уровне ведущую роль играют Госсовет КНР, министерства и ведомства.

Ключевым элементом в системе нормативных правовых актов, посвященных электронной торговле, является Закон КНР «Об электронной коммерции» [12]. Он закрепляет правовой статус платформ электронной коммерции, устанавливает гарантии для потребителей, вводит базовые правила по досудебному урегулированию споров, вытекающих из сделок, заключенных на платформе.

Госсовет КНР активно регулирует сферу e-commerce. Так, им приняты Руководящие мнения по содействию здоровому и быстрому развитию трансграничной электронной коммерции 2015 г. [13]. Антимонопольной комиссией Госсовета КНР издано «Антимонопольное руководство по платформенной экономике» [1], в котором содержатся критерии, позволяющие определить доминирующее положение платформы электронной коммерции и злоупотребление им, в том числе при помощи различного рода алгоритмов, осуществляющих координацию цен и других условий договоров без вмешательства человека.

Большое влияние на развитие отдельных сфер электронной коммерции оказывает нормотворчество министерств и ведомств КНР. Так, Министерством транспорта введены дополнительные требования к платформам электронной коммерции,

осуществляющим прием онлайн-заказов такси. Они изложены во «Временных мерах для администрирования бизнес-операций и услуг по онлайн-бронированию такси» [3]. Данный нормативный правовой акт, например, предписывает платформам проверять техническое состояние транспортных средств и квалификацию водителей. Примером еще одного министерского акта является Уведомление «О налоговой политике в отношении розничного экспорта в Трансграничных комплексных пилотных зонах электронной торговли» [10], которым отменен налог на добавленную стоимость для предприятий электронной коммерции, имеющих статус резидентов указанных зон. Как видно из изложенного выше, министерства и ведомства не только уточняют положения Закона «Об электронной коммерции», но и вводят дополнительные обязанности, права и преференции для участников рынка.

Власти провинций и городов уполномочены устанавливать различного рода льготы и субсидии для предприятий электронной коммерции. Например, Народным правительством г. Пекина [7] утвержден комплекс мер поддержки, способствующих развитию пилотной зоны трансграничной электронной торговли в данном городе.

Существующий в КНР подход регулирования электронной коммерции подвергается критике исследователями, указывающими на то, что на государственном уровне необходимо разработать единые и стандартизированные законы и нормативные акты, чтобы исключить возможные противоречия [4]. Однако нельзя не отметить, что существующая модель позволяет регионам активно поддерживать организации развивающие электронную коммерцию [17], защищать права потребителей и внутриплатформенного бизнеса, снижать нагрузку на судебную систему.

Законодательство России об электронной коммерции. Как уже отмечалось, в России отсутствует специальный нормативный правовой акт, касающийся электронной торговли. Однако действуют законы, создающие инфраструктуру для развития электронной коммерции, например, Федеральный закон «О национальной платежной системе» [11]. Непосредственно вопросы функционирования платформ электронной коммерции регулирует Закон Российской Федерации «О защите прав потребителей» [9], который дает определение владельца агрегатора информации о товарах (услугах), устанавливает обязанности оператора платформы и случаи его ответственности перед потребителем (ст. 9, 12, 16).

Еще одним источником регулирования электронной коммерции, а именно трансграничной электронной торговли, является Федеральный закон «О внесении изменения в статью 120 Федерального закона «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» [8]. Закон уполномочивает Правительство Российской Федерации на проведение эксперимента по совершению таможенных операций назначенным оператором почтовой связи с применением таможенной процедуры таможенного склада в отношении товаров, ввозимых в Россию в целях последующего приобретения физическими лицами в рамках международной электронной торговли. Принятие данного закона позволило реализовать концепцию по созданию бондовых складов, о пользе которых говорят исследователи [2]. Данный шаг должен снизить уровень проблем с логистикой, которые, как справед-

ливо отмечается в литературе, являются ключевыми в деле развития трансграничной электронной коммерции [5].

Таким образом, в России отношения в сфере электронной коммерции урегулированы частично. Законодательство уделяет внимание лишь защите прав потребителей, приобретающих товары и услуги на платформах электронной коммерции, в то время как отсутствуют какие-либо гарантии для внтриплатформенного бизнеса, позволяющие исключить вмешательство в его деятельность самих платформ. Кроме того, нельзя также утверждать, что в полной мере решены вопросы привлечения оператора платформы к ответственности за продаваемые при ее помощи некачественные товары (услуги). Также отсутствуют нормативные правовые акты, содержащие меры для стимулирования российских производителей развивать экспортный потенциал трансграничной электронной торговли.

Заключение. Для России закон об электронной коммерции необходим, так как его наличие позволит обеспечить права всех участников данной сферы, равно как и снизить вероятность злоупотреблений со стороны операторов платформ. При разработке отечественного закона следует использовать опыт КНР в следующих сферах: обеспечение информирования потребителей о качестве товаров и услуг; мониторинг платформой электронной коммерции качества товаров и услуг, реализуемых на ней; антимонопольное регулирование деятельности операторов платформ; внесудебное урегулирование споров на платформе; защита персональных данных пользователей платформ. Учитывая китайский опыт, важно также разработать комплекс мер поддержки для развития российской трансграничной торговли.

Список литературы

1. Антимонопольное руководство по платформенной экономике [国务院反垄断委员会关于平台经济领域的反垄断指南] от 07.02.2021. Портал Государственного Совета КНР. URL: http://www.gov.cn/xinwen/2021-02/07/content_5585764.htm (дата обращения: 10.09.2022).

2. Ворона А. А., Дианова В. Ю. Регулирование трансграничной (внешней) электронной торговли как фактор развития товарооборота // Таможенное дело. 2022. № 1. С. 25–30.

3. Временные меры для администрирования бизнес-операций и услуг по онлайн-бронированию такси [网络预约出租汽车经营服务管理暂行办法] от 28.07.2016. Портал Государственного Совета КНР. URL: http://www.gov.cn/xinwen/2016-07/28/content_5095584.htm (дата обращения: 10.09.2022).

4. Вэй Д., Чжан Ц. D. Достижения и перспективы Создания Комплексной пилотной зоны трансграничной электронной торговли в Китае // Интертрейд. 2019. № 7. С. 18. [韦大宇, 张建民. 中国跨境电商综合试验区建设成果与展望 // 贸易经济].

5. Гончарук И. В. Управление цепями поставок в трансграничной торговле: новое в российской практике // Научные труды Северо-Западного института управления РАНХиГС. 2021. Т. 12. № 4 (51). С. 72–79.

6. Доля продаж через Интернет в общем объеме оборота розничной торговли // ЕМИСС. URL: https://www.fedstat.ru/indicator/50236 (дата обращения: 10.09.2022).

7. Комплексный план внедрения пилотной зоны трансграничной электронной торговли в Китае (Пекин): уведомление Главного управления Пекинского муниципального народного правительства [北京市人民政府办公厅关于印发中国(北京)跨境电子商务综合试验区实施方案的通知] от 18.12.2018. Народное Правительство г. Пекин. URL: http://www.beijing.gov.cn/zhengce/zhengcefagui/201905/t20190522_61765.html (дата обращения: 10.09.2022).

8. О внесении изменения в статью 120 Федерального закона «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»: Федеральный закон от 14.07.2022 № 314-ФЗ // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202207140105 (дата обращения: 10.09.2022).

9. О защите прав потребителей: Закон РФ от 07.02.1992 № 2300–1 (ред. от 14.07.2022) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_305/ (дата обращения: 10.09.2022).

10. О налоговой политике в отношении розничного экспорта в Трансграничных комплексных пилотных зонах электронной торговли: Уведомление Министерства финансов, Государственного налогового управления, Министерства торговли и Главного таможенного управления [财政部、税务总局、商务部、海关总署关于跨境电子商务综合试验区零售出口货物税收政策的通知] от 28.09.2018. Информационный центр правовой системы Пекинского университета. URL: https://pkulaw.com/chl/5d0ba302bc523463bdfb.html (дата обращения: 10.09.2022).

11. О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 14.07.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 10.09.2022).

12. Об электронной коммерции: Закон КНР [中华人民共和国电子商务法] от 31.08.2018 № 7. Портал Министерства коммерции КНР. URL: http://www.mofcom.gov.cn/article/zt_dzswf/deptReport/201811/20181102808398.shtml (дата обращения: 10.09.2022).

13. Руководящие мнения по содействию здоровому и быстрому развитию трансграничной электронной коммерции [国务院办公厅关于促进跨境电子商务健康快速发展的指导意见] от 16.06.2015 // lawinfochina.com. URL: http://www.lawinfochina.com/display.aspx?id=26592&lib=law&EncodingName=big5 (дата обращения: 10.09.2022).

14. Суворов Е. Д. Некоторые проблемы электронной торговли: к вопросу об ответственности владельцев агрегаторов перед потребителями // Вестник экономического правосудия Российской Федерации. 2019. № 9. С. 57–67.

15. Шевченко Г. Н., Моисейцев В. В. Альтернативные методы решения споров в электронной коммерции // Бизнес, менеджмент и право. 2022. № 2 (54). С. 27–31.

16. Яо Биюй. Система законодательства об электронной коммерции в Китайской Народной Республике // Конкурентное право. 2022. № 1. С. 27–30.

17. Alekseenko A. Legal Regulation of China's Cross-border E-Commerce Comprehensive Pilot Areas: A Russian Perspective // China & WTO Review. 2022. № 1. Pp. 7–28.

18. E-commerce и взаимосвязанные области (правовое регулирование): сборник статей / А. А. Богустов, О. Н. Горохова, Д. А. Доротенко и др.; рук. авт. кол. и отв. ред. М. А. Рожкова. Москва: Статут, 2019. 448 с.

19. E-commerce in China – statistics & facts // Statista.com. URL: https://www.statista.com/topics/1007/e-commerce-in-china/#topicHeader__wrapper (дата обращения: 10.09.2022).

20. Retail e-commerce sales CAGR from 2022 to 2025, by country // Statista.com. URL: https://www.statista.com/forecasts/220177/b2c-e-commerce-sales-cagr-forecast-for-selected-countries (дата обращения: 10.09.2022).

З. А. Ашуров,
доктор философии по экономическим наукам (PhD),
старший научный сотрудник,
Центр исследования проблем приватизации и управления
государственными активами
при Агентстве по управлению государственными
активами Республики Узбекистан

ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ ПРАВОВЫХ ОСНОВ ЭЛЕКТРОННОЙ КОММЕРЦИИ В УЗБЕКИСТАНЕ ПРИ РЕГУЛИРОВАНИИ ЦИФРОВИЗАЦИИ ЭКОНОМИЧЕСКИХ ОТНОШЕНИЙ

Аннотация. В данной статье рассматриваются вопросы совершенствования правовых основ электронной коммерции в Узбекистане. Целью исследования является изучение действующей нормативно-правовой базы в сфере электронной коммерции и выработка рекомендаций для ее совершенствования с целью усиления регулирования процессов цифровизации экономических отношений. Для этого автором статьи на основе изучения действующей законодательной базы в сфере электронной коммерции были выявлены проблемы и необходимость совершенствования законодательной базы электронной коммерции и по итогам даны предложения и рекомендации, которые могут быть учтены при разработке проекта Закона «Об электронной коммерции» в новой редакции.

Ключевые слова: право, правовые основы, законодательство, электронная коммерция, цифровизация, цифровая экономика, цифровые технологии, экономические отношения

THE ISSUES OF IMPROVING THE LEGAL FRAMEWORK OF E-COMMERCE IN UZBEKISTAN IN REGULATION OF DIGITALIZATION OF ECONOMIC RELATIONS

Abstract. This paper discusses the issues of improving the legal framework of e-commerce in Uzbekistan. The purpose of the research is study the current regulatory framework in the field of e-commerce, and to develop the recommendations for its

improvement in order to strengthen the regulation of the processes of digitalization of economic relations. For this, the author of the paper, based on the study of the current regulatory basis in the field of e-commerce, identified problems and need to improve the legislative framework for e-commerce, and, as a result, gave his proposals and recommendations which should be taken into account when working out the revised draft Law "On E-commerce".

Keywords: Law, Legal framework, Legislation, E-commerce, Digitalization, Digital economy, Digital technologies, Economic relations

Сегодня в Узбекистане реализуются комплексные меры по активному развитию цифровой экономики, а также широкому внедрению современных информационно-коммуникационных технологий во все отрасли и сферы, прежде всего, в государственное управление, образование, здравоохранение и сельское хозяйство. В частности, начата реализация свыше 220 приоритетных проектов, предусматривающих совершенствование системы электронного правительства, дальнейшее развитие информационно-коммуникационных технологий, повышение цифровой грамотности и навыков, цифровизацию экономических отношений и социальной сферы. В целях ускоренного развития цифровой индустрии в республике и повышения конкурентоспособности национальной экономики Указом Президента Республики Узбекистан от 5 октября 2020 г. № УП-6079 [2] утверждена Стратегия «Цифровой Узбекистан – 2030», согласно которой для совершенствования нормативно-правовой базы цифровизации экономических отношений предусмотрена разработка проекта Закона Республики Узбекистан «Об электронной коммерции» в новой редакции.

Как нам известно, развитие любой сферы требует адаптации и совершенствования ее правовых основ к новым реалиям. В частности, внедрение информационно-коммуникационных технологий в экономику и процесс цифровизации ведут к расширению масштабов электронной коммерции в торговых отношениях. Согласно некоторым данным, объем валового производства в сфере электронной коммерции за последние пять лет увеличился в 48 раз [3]. Кроме того, глобальная пандемия увеличила потребность в электронной коммерции среди населения мира. В результате система онлайн-торговли растет с каждым годом. Только в 2020 г. объем продаж через электронную коммерцию увеличился на 24,9 % в Китае, на 25,9 % в Южной Корее, на 14 % в США и на 11,7 % в Сингапуре. За этот период объем электронной коммерции в Узбекистане вырос на 80 % [1].

Такая ситуация выдвинула на повестку дня вопросы совершенствования правовых основ электронной коммерции, действующих с 2015 г., и разработки Закона «Об электронной коммерции» в новой редакции, который сейчас обсуждается парламентариями Узбекистана. Поскольку действующий закон не распространяется на все субъекты электронной коммерции, он вызывает недопонимание в применении правил обмена документами электронной коммерции, механизмов оплаты и возврата товаров, а также приводит к провалу его применения.

На наш взгляд, в нынешних условиях необходимость совершенствования правовых основ электронной коммерции обусловлена следующим:

– *во-первых*, система правового регулирования отношений в области электронной коммерции не соответствует быстро меняющимся тенденциям развития отрасли, что не позволяет обеспечить доступность электронной коммерции широким слоям населения и субъектам предпринимательства;

– *во-вторых*, действующий закон не предусматривает предоставление определений терминов, используемых в области электронной коммерции;

– *в-третьих*, действующий закон не определяет принципы направления государственной политики в области электронной коммерции, а также в должной мере не раскрывает роль государственных органов в развитии электронной коммерции;

– *в-четвертых*, в действующем законе не определены роли всех субъектов электронной коммерции, например, не определены требования к операторам торговых платформ и субъектам, осуществляющим доставку товаров;

– *в-пятых*, существующие законодательные акты не в полном объеме раскрывают вопросы обмена документами, механизмов оплаты и возврата товаров в электронной коммерции;

– *в-шестых*, действующий закон несет рамочный характер, а конкретные механизмы взаимодействия определены в разных подзаконных актах, что в целом свидетельствует о фрагментации регулирования сферы электронной коммерции.

Считаем, что при разработке проекта Закона «Об электронной коммерции» в новой редакции (далее – проект закона) в нем должен найти отражение ряд важных норм. К примеру, на практике существуют общие требования к заключению электронных договоров, но их особенности не регламентированы. В проекте закона необходимо уточнять условия заключения электронных договоров, конкретный порядок заключения электронной сделки, юридическую силу электронных документов, требования к оферте, особенности хранения электронных документов, внедрение порядка увеличения электронных сделок. Также необходимо в электронной коммерции внедрить систему денежного депозита (эскроу), которая позволяет хранить деньги в информационной системе до полного выполнения условий покупателя.

Помимо юридических лиц, право участия в электронной коммерции также нужно предоставлять и самозанятым физическим лицам. Действующий закон определяет только права и обязанности продавцов, но покупатель также должен иметь ряд прав. Следовательно, в проекте закона целесообразно предусмотреть, чтобы покупатель мог приобретать товары (работы, услуги) путем заключения договоров, получать полную информацию о товарах (работах, услугах), производителе и других условиях приобретения товаров (работ, услуг), условиях за участие в операциях, проводимых в сфере электронной коммерции, требовать равноправия и защиты своих прав и законных интересов.

Важно установить, что продавец (поставщик услуг или исполнитель работ) вправе организовать собственную электронную торговую площадку и осуществлять непосредственную реализацию товаров (работ, услуг) на ней, а также не осуществлять продажу товаров или оказание услуг, запрещенных законодательством. В электронной коммерции договор должен оформляться посредством электронных документов или обмена сообщениями между сторонами, путем согласования

условий сделки и создания электронного документа. Договор в электронной торговле не может быть признан недействительным только на основании того, что он заключен с использованием информационных систем.

При установлении требований к заключению договоров необходимо определить, что чеки, квитанции, сообщения и другие документы в электронном виде, позволяющие операторам или продавцам электронной коммерции идентифицировать стороны договора, приравниваются к аналогичным документам на бумажном носителе, подтверждающим покупку товаров (работы, услуги). В случаях, когда законом или соглашением сторон требуется собственноручное подписание документа при заключении договоров, электронный документ необходимо считать подписанным, если стороной договора осуществлена процедура подтверждения электронной цифровой подписи. В качестве подписи в документе электронной коммерции также необходимо признать такие методы электронного подтверждения, как СМС, Face-ID и др.

Необходимо отметить, что механизмы экспорта и импорта цифровых товаров и услуг в сфере электронной коммерции не регулируются действующим законодательством, а это создает барьеры для их продажи. Поэтому в проекте закона необходимо определить особенности экспорта и импорта цифровых продуктов (любых товаров, созданных в цифровом виде, например, операционных систем, программного обеспечения, онлайн-сервисов и т. п.), ввести порядок таможенного оформления (декларирования). Считаем, что цифровые товары, экспортируемые или импортируемые методами цифровой дистрибуции, не должны проходить таможенную очистку.

Учитывая, что сейчас имеется множество современных цифровых платежных технологий, платежи в электронной коммерции должны осуществляться разными способами: во-первых, наличными деньгами путем предоставления покупателю подтверждающих документов о приеме наличных денег в виде платежного средства, осуществленных через виртуальные терминалы («E-POS»); во-вторых, посредством перевода денежных средств с банковского счета, в том числе через персональный кабинет или через систему платежной организации; в-третьих, с использованием электронных денег посредством перевода средств электронного кошелька, открытого в системе электронных денег.

В заключение хотели бы отметить, что принятие нового и усовершенствованного законодательства об электронной коммерции в Узбекистане даст возможность расширению спектра новых методов электронной коммерции путем формирования условий эффективной конкуренции субъектов предпринимательства на внутреннем и международном рынках, увеличению экспортного потенциала страны и развитию международного сотрудничества в сфере электронной коммерции, дальнейшему внедрению передовых информационных технологий, новых инструментов регулирования отношений в сфере электронной коммерции. Полагаем, что также будут устранены излишние бюрократические барьеры на пути развития предпринимательства в сфере электронной коммерции, улучшена деловая среда и будут созданы дополнительные рабочие места.

Список литературы

1. Гадоев Э. Электрон тижоратда янги инновацион усуллар [Новые инновационные методы в электронной коммерции] // Биржа. Экономическая газета. 2022. № 72 (2955). С. 2.

2. Закон «Об электронной коммерции» расширяет возможности в этой области. 13.09.2022. URL: https://yuz.uz/ru/news/zakon-ob-elektronnoy-kommertsii-rasshiryaet-vozmojnosti-v-etoy-oblasti (дата обращения: 16.09.2022).

3. Об утверждении Стратегии «Цифровой Узбекистан – 2030» и мерах по ее эффективной реализации: Указ Президента Республики Узбекистан от 5 октября 2020 года № УП-6079 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/docs/5031048 (дата обращения: 16.09.2022).

А. А. Белецкая,
старший преподаватель кафедры
трудового и предпринимательского права,
Белгородский государственный
национальный исследовательский университет
О. С. Фефелов,
инженер-программист,
Белгородский государственный
национальный исследовательский университет

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ МАРКЕТПЛЕЙСОВ С ПОТРЕБИТЕЛЯМИ (НА ПРИМЕРЕ «АВИТО»)

Аннотация. Современное правовое регулирование обязательств по купле-продаже товаров претерпевает существенные изменения в связи с развитием форм и способов совершения сделок и передачи вещей, развития цифровых технологий. Однако подчас фактически сложившиеся общественные отношения опережают их правовую регламентацию. Такую ситуацию можно наблюдать и при продаже товаров через маркетплейсы. В данной статье будут рассмотрены особенности участия маркетплейса «Авито» и его банка-партнера («Тинькофф Банк») в совершении сделок, а также некоторые аспекты защиты прав покупателей и продавцов товаров. Также проведено сравнение фактически складывающихся отношений между маркетплейсом, банком-партнером, продавцами и покупателями с юридически закрепленной конструкцией инвестирования с использованием инвестиционных платформ (краудфандингом).

Ключевые слова: пользование чужими денежными средствами, удержание, ответственность, защита прав потребителей, переход права собственности, цифровые технологии, краудфандинг

LEGAL REGULATION OF RELATIONS OF MARKETPLACES WITH CONSUMERS (BY THE EXAMPLE OF "AVITO")

Abstract: modern legal regulation of obligations for the purchase and sale of goods is undergoing significant changes in connection with the development of forms and methods of transactions and the transfer of things, the development of digital technologies. However, sometimes, the actually established social relations are ahead of their legal regulation. This situation can also be observed when selling goods through marketplaces. This article will discuss the features of the participation of the Avito marketplace and its partner bank (Tinkoff Bank) in transactions, as well as some aspects of protecting the rights of buyers and sellers of goods. Also, a comparison was made of the actually developing relations between the marketplace, the partner bank, sellers and buyers with a legally fixed investment structure using investment platforms (crowdfunding).

Keywords: Use of other people's money, Retention, Responsibility, Consumer protection, Transfer of ownership, Digital technologies, Crowdfunding

Введение. В современном капиталистическом обществе следствием компьютеризации является рост безработицы. Усиление эксплуатации «нервной энергии» интеллигенции и рабочих, повышение прибылей национальных и транснациональных корпораций, ускорение гонки вооружений, усиление контроля за личной и общественной жизнью граждан. Несмотря на то, что в современном мире множество договоров купли-продажи товаров заключаются уже не в устной или простой письменной форме, традиционно использовавшихся ранее и предусмотренных Гражданским кодексом Российской Федерации, а посредством обмена электронными документами, направления оферты и получения акцепта посредством передачи сообщений в мессенджерах, ввода информации в определенные формы на сайтах в сети Интернет, актуальным по-прежнему остается вопрос защиты прав потребителей – приобретателей товаров, работ, услуг. Популярность интернет-площадок вполне объяснима в современных реалиях экономии времени, стремлении все успеть, однако потребителям не стоит расслабляться, поскольку с развитием цифровых технологий наблюдается развитие и способов мошенничества. Одной из таких интернет-площадок, маркетплейсом, о котором в данной статье пойдет речь, является «Авито».

Как справедливо отмечает Е. Б. Подузова, условия использования «Авито» являются практическим примером фактического (но не юридического) взаимодействия пользователя и правообладателя программного обеспечения при оказании услуг в цифровой среде [6. С. 63].

Основная часть. Порядок взаимодействия продавца и покупателя посредством маркетплейса «Авито» выглядит следующим образом.

Покупатель, выбрав товар на платформе, кликая на кнопку заказа, запускает процедуру оформления покупки и доставки. Со счета покупателя в этот момент списываются денежные средства и зачисляются на счет банка-партнера («Тинькофф Банк»). Далее осуществляется доставка товара покупателю, занимающая какое-то количество дней. И только после получения покупателем товара

банк-партнер осуществляет транзакцию – перевод списанных со счета покупателя денежных средств на счет продавца. Причем поступление средств на счет может происходить не за один день. Возникает закономерный вопрос: является ли пользование денежными средствами банком-партнером законным? Ведь подчас с момента их списания со счета покупателя до момента зачисления на счет продавца может проходить большой промежуток времени. Ни федеральное законодательство, ни правила взаимодействия банка-партнера с «Авито», ни договор оферты, который предлагает этот маркетплейс, не регламентируют возможность либо невозможность банка пользоваться временно свободными денежными средствами, поступающими от продавца, до момента перечисления их на счет покупателю.

На наш взгляд, вопрос о правомерности такого пользования должен быть разрешен с учетом общих положений ГК РФ в силу отсутствия специального правового регулирования.

Рассмотрим правовое регулирование складывающихся общественных отношений, для этого обратимся к ГК РФ.

Согласно ч. 1 ст. 223 ГК РФ право собственности у приобретателя вещи по договору возникает с момента ее передачи, если иное не предусмотрено законом или договором [2]. То есть при покупке товара посредством маркетплейса «Авито» право собственности на вещь будет возникать у покупателя в момент ее передачи. А так как по большей части товары посредством такой купли-продажи пересылаются по всей стране, следует помнить и о положениях ч. 1. ст. 224 ГК РФ, согласно которой передачей признается вручение вещи приобретателю, а равно сдача перевозчику для отправки приобретателю или сдача в организацию связи для пересылки приобретателю вещей, отчужденных без обязательства доставки [2].

На самом деле, даже если бы заключение договора сложно было доказать, учитывая специфику оформления этого процесса в данных обстоятельствах, такая передача вещей все равно является частью гражданского оборота, так как оба лица – передающее и принимающее – выступают по отношению друг к другу в качестве самостоятельных хозяйствующих субъектов и в случае нарушения правил передачи, затрагивающих их имущественные права, они могут прибегнуть к защите этих прав в исковом порядке в арбитраже.

Вещь считается врученной приобретателю с момента ее фактического поступления во владение приобретателя или указанного им лица.

Получается, что право собственности на товар возникает у покупателя уже в момент передачи его в почтовое отделение либо любой организации, осуществляющей доставку. Однако же денежные средства, уплаченные за товар, будут находиться на банковском счете еще в течение всего периода доставки.

Помним, что банк, согласно ст. 1 Федерального закона от 02.12.1990 № 395–1 (ред. от 14.07.2022) «О банках и банковской деятельности», – это кредитная организация, которая имеет исключительное право осуществлять в совокупности следующие банковские операции: привлечение во вклады денежных средств физических и юридических лиц, размещение указанных средств от своего имени и за свой счет на условиях возвратности, платности, срочности, открытие и ведение банковских счетов физических и юридических лиц [4].

И более конкретно – перечень банковских операций в пп. 3 и 4 ст. 5 указанного Закона: «…открытие и ведение банковских счетов физических и юридических лиц; осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам» и множество других операций, осуществляемых в рамках коммерческой деятельности банков [4].

Банк, по определению, – кредитная организация, а у кредитной организации основная цель деятельности – извлечение прибыли.

Здесь опять считаем возможным обратиться к ГК РФ для сопоставления определения предпринимательской деятельности с деятельностью банков. Согласно ч. 1 ст. 2 ГК РФ предпринимательской является самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг [2].

Логичным представляется, что, «завладев» на время свободными денежными средствами, банк-партнер не просто хранит их на счете, а всячески распоряжается, извлекая прибыль.

Не менее логичным представляется и предположение, что все эти действия и маркетплейса, и банка-партнера по некоторым признакам, содержание которых мы сейчас обозначим, подпадают под действия Закона «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» от 02.08.2019 № 259-ФЗ. Краудфандинг обычно относится к методу финансирования, при котором деньги собираются путем привлечения вкладов большого количества людей [1. С. 2].

По сути, «Авито» на сегодняшний день превращается в своеобразную инвестиционную цифровую платформу. Да и в целом взаимодействие участников хозяйственной деятельности через цифровые платформы расширяется.

Согласно положениям ст. 2 Закона «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» [5], оператор инвестиционной платформы должен быть включен Банком России в реестр операторов инвестиционных платформ, т. е. зарегистрирован в установленном законом порядке. Конечно же, маркетплейс «Авито», де-юре осуществляя деятельность по организации привлечения инвестиций, де-факто не регистрируется в указанном порядке. При этом Банк России не осуществляет в отношении него никаких контрольных функций. Банк-партнер, в данном случае «Тинькофф Банк», фактически выступает в рассматриваемых отношениях как лицо, привлекающее инвестиции, т. е. как лицо, которому оператор инвестиционной платформы оказывает услуги по привлечению инвестиций, а покупатель – как инвестор – лицо, которому оператор инвестиционной платформы оказывает услуги по содействию в инвестировании.

Таким образом, мы можем наблюдать деятельность, фактически подпадающую под инвестирование с использованием инвестиционных платформ, причем такой краудфандинг носит незаконный характер.

Теперь обратимся к локальным правилам, называющимся «Условия Авито Доставки», размещенным на официальном сайте «Авито» (https://www.avito.ru/legal/goods/delivery).

Заказ считается оформленным после его успешной оплаты и резервирования банком денежных средств по заказу. В случае непредоставления продавцом данных действительной банковской карты для выплаты банком денежных средств покупателя за товар в течение семи дней с момента получения уведомления от компании денежные средства могут быть возвращены покупателю.

При получении отправления в ПВЗ или у курьера покупатель обязан проверить товар на предмет соответствия товара описанию в объявлении (осмотреть товар) в присутствии представителя службы доставки. Если покупатель обнаружит недостатки товара, например, несоответствие товара описанию в объявлении, наличие повреждений, дефектов и т. п., он вправе до приемки отправления отказаться от товара и передать отправление представителю службы доставки для его возврата продавцу [8].

Так как все банковские операции в данном случае осуществляются через банк-партнер «Авито» – «Тинькофф Банк», обратимся к его внутренним актам, регулирующим порядок взаимодействия с маркетплейсом. На этот счет действует Договор публичной оферты «Об условиях предоставления АО “Тинькофф Банк” услуг по оплате и переводам с банковских карт в рамках онлайн сервисов “Авито” (далее – Оферта)», размещенный на официальном сайте в свободном доступе.

Остановимся на анализе пунктов 2.6.3, 2.6.4, 2.8 указанной оферты:

«2.6.3. Перечисление средств Покупателя на Карту получателя (Продавца) в размере суммы стоимости Товара/Услуг аренды за вычетом стоимости Услуги Сервиса для Продавца осуществляется в день получения Банком информации от “Авито” о необходимости осуществления такого перечисления. Для перечисления средств Покупателя на Карту получателя (Продавца) “Авито” направляет указанную информацию Банку в момент подтверждения Покупателем факта принятия Товара, подтверждения факта принятия Покупателем Помещения или отказа Покупателя от аренды Помещения, произведенного в сроки и в порядке, предусмотренные условиями Соглашения “Авито”».

Подобные формулировки, на наш взгляд, под видом заботы об интересах покупателя на самом деле приводят к легализации возможности обогащения банка-партнера. Покупатель фактически, помимо стоимости товара, обозначенной продавцом, оплачивает услуги сервиса, а продавец вынужден ждать заработанных им денег подчас неоправданно долго. При этом разъяснений, что в себя включают услуги сервиса, в документе нет.

«2.6.4. Осуществление полного или частичного возврата средств Покупателя на Карту отправителя (Покупателя), ранее списанных с Карты отправителя (Покупателя), осуществляется в день получения Банком информации от “Авито” о необходимости осуществления такого возврата. “Авито” направляет указанную информацию Банку в момент отказа Продавца от предоставления Товара в пункте приема Товара для осуществления Доставки, а также в момент отказа Покупателя от Товара полностью или частично или отказа Покупателя от аренды Помещения, произведенного в сроки и в порядке, предусмотренными условиями Соглашения “Авито”».

То есть механизмы защиты прав и продавца, и покупателя все-таки существуют, но они никак не связаны с моментом исполнения банком-партнером своих

обязательств по перечислению средств. Не стоит забывать в этой ситуации и о регулировании подобных моментов на уровне ГК РФ.

«2.8. Клиент соглашается с тем, что Банк не несет ответственности за направление “Авито” информации (в том числе за сроки направления “Авито” такой информации), необходимой для совершения Банком действий, предусмотренных п. 2.6, а также п. 3.4.1 Договора. Со всеми претензиями о ненадлежащем или несвоевременном направлении “Авито” информации Банку Клиент должен обращаться в “Авито”» [9]. На наш взгляд, чем длиннее цепочка взаимодействий и чем больше в ней участников, тем сложнее конечному потребителю будет реализовывать в полном объеме принадлежащие ему по закону права.

Используя «Авито Доставку», продавец получает деньги только тогда, когда доставка подтвердится, а покупатель примет товар и распишется, что не имеет к нему претензий. До этого момента «Авито» хранит деньги покупателя и выступает в роли гаранта [3]. Утверждение о роли гаранта не подкреплено ссылками во внутренних анализируемых актах на положения соответствующего договора в ГК РФ. При этом остается еще открытым вопрос взаимодействия «Авито» и банка-партнера в части получения и перераспределения денежных средств покупателей. Но в силу того, что статья носит обзорный характер и касается взаимодействия сторон в рамках действия гражданско-правовых норм, предметом исследования он являться не будет.

Заключение. Современную жизнь трудно представить без использования множества различных высокотехнологичных устройств: мобильных телефонов, планшетов, компьютеров, пластиковых карт. Уже сейчас существует техническая возможность хранить в памяти компьютеров практически всю накопленную человечеством информацию и использовать ее для решения экономических, технологических, социальных и культурных задач. Происходит формирование программ искусственного интеллекта, способных производить ряд рациональных познавательных процедур, свойственных человеческому мышлению. Постоянно появляются новые сервисы и программное обеспечение. Все перечисленное, делая нашу жизнь удобнее, при этом требует определенных знаний и навыков [7. С. 172]. В силу этого требуется современное правовое регулирование фактически сложившихся общественных отношений в рассмотренной сфере.

На основании всего вышеизложенного предлагаем обязать банк перечислять денежные средства на счет продавца в момент передачи товара, т. е., руководствуясь положениями ст. 224 ГК РФ, в момент передачи вещи для доставки организации связи под угрозой применения санкций, предусмотренных ст. 395 ГК РФ «Ответственность за неисполнение денежного обязательства».

Согласно ч. 1 ст. 395 ГК РФ, в случаях неправомерного удержания денежных средств, уклонения от их возврата, иной просрочки в их уплате подлежат уплате проценты на сумму долга. Размер процентов определяется ключевой ставкой Банка России, действовавшей в соответствующие периоды. Эти правила применяются, если иной размер процентов не установлен законом или договором [2].

Таким образом, в законодательстве нет каких-либо ограничений на осуществление банком-партнером возможности свободно пользоваться временно разме-

щенными в нем денежными средствами покупателя товаров. Видимых угроз для покупателя это не представляет, однако приводит к неправомерному обогащению банков и маркетплейсов.

Представляется, что в условиях санкционного давления, сохранения неопределенности с поставками оборудования и отключением от иностранной ИТ-инфраструктуры, возникает необходимость обеспечения российских граждан привычными интернет-сервисами и каналами взаимодействия. Так как в настоящее время в значительной степени ограничена работа иностранных магазинов приложений (Google Play, AppStore), имеется риск прекращения их работы в Российской Федерации, имеет смысл налаживать работу отечественных маркетплейсов. Однако в условиях противодействия санкциям со стороны иностранных государств необходимо не только стремиться обеспечить безотказность и исправность оказания российским гражданам интернет-сервисов, различного рода услуг, но и заботиться о качестве их предоставления, а также о соблюдении гражданского законодательства и законодательства о защите прав потребителей.

Список литературы

1. Beletskaia A. A., Goncharova L. N., Sinenko V. S., Khlebnikov A. D., Sorokoletova M. S. Legal Regulation of Crowdfunding in Russia and Foreign Countries // Turismo: Estudos & Práticas (UERN), Mossoró/RN, Caderno Suplementar 03, 2020. URL: http://natal.uern.br/periodicos/index.php/RTEP [ISSN 2316–1493].

2. Гражданский кодекс Российской Федерации (часть первая) (статьи 1–453) (с изменениями на 28 июня 2022 года). № 51-ФЗ // Российская газета, № 238–239, 08.12.1994.

3. На Avito появилась Доставка. Как ей вообще пользоваться? URL: https://www.iphones.ru/iNotes/789299 (дата обращения: 12.09.2022).

4. О банках и банковской деятельности: ФЗ № 395–1 (в редакции Федерального закона от 3 февраля 1996 года № 17-ФЗ) (с изменениями на 14 июля 2022 года) (редакция, действующая с 25 июля 2022 года) // Собрание законодательства Российской Федерации. № 6. 05.02.96. Ст. 492.

5. О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 2 августа 2019 г. № 259-ФЗ // Российская газета. 7 августа 2019 г. № 172.

6. Подузова Е. Б. Договоры об оказании услуг в сфере использования «искусственного интеллекта» и технологий «искусственного интеллекта»: проблемы теории и практики // Актуальные проблемы российского права. 2022. Т. 17, № 8. С. 59–67. DOI: 10.17803/1994–1471.2022.141.8.059–067

7. Смагоринский Б. П., Сычева А. В. О некоторых актуальных способах совершения мошенничества в отношении физических лиц в современных условиях // Вестник Волгоградской академии МВД России. 2022. № 2 (61). URL: https://cyberleninka.ru/article/n/o-nekotoryh-aktualnyh-sposobah-sovershheniya-moshennichestva-v-otnoshenii-fizicheskih-lits-v-sovremennyh-usloviyah (дата обращения: 12.09.2022).

8. «Условия Авито Доставки», размещенные на официальном сайте Авито. URL: https://www.avito.ru/legal/goods/delivery (дата обращения: 12.09.2022).

9. Публичная оферта об условиях предоставления АО «Тинькофф Банк» услуг по оплате и переводам с банковских карт в рамках онлайн-сервисов Авито. URL: https://emirsaba.org/publichnaya-oferta.html (дата обращения: 12.09.2022).

В. А. Белов,
кандидат юридических наук,
доцент кафедры предпринимательского и корпоративного права,
Российский государственный университет правосудия

ПРАВО И НЕПРАВО В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ПОТРЕБИТЕЛЬСКИХ ПРАВООТНОШЕНИЙ

Аннотация. Цифровизация повседневных активностей ставит определенные вызовы перед правом и регулированием общественных отношений, в том числе возникающих с участием потребителей. В рамках настоящей статьи ставится цель по обоснованиям того, что в условиях цифровизации общественных отношений, в том числе с участием потребителей, классические теории правопонимания не в полной степени способствуют регулированию фактически складывающихся отношений, а интегративная теория правопонимания позволяет избежать текущих проблем в сфере правоприменительной и судебной практики, возникающих в цифровой среде. Также предпринята попытка формулирования специальных принципов для потребительских правоотношений, позволяющих наиболее успешно рассматривать фактически возникающие вопросы и споры с участием потребителей, в результате совершения ими действий в цифровой среде.

Ключевые слова: правопонимание, цифровизация, интегративная теория, потребительские правоотношения, принципы права, потребитель, пробелы в законе, ошибочная судебная практика, диджитализация, цифровая среда

RIGHT & UNRIGHT IN CONDITIONS OF DIGITALIZATION OF CONSUMER RELATIONSHIPS

Abstract. The digitalization of everyday activities poses certain challenges to the law and regulation of social relations, including those arising with the participation of consumers. Within the framework of this article, the goal is to substantiate the fact that in the context of digitalization of public relations, including with the participation of consumers, classical theories of law understanding do not fully contribute to the regulation of actually developing relations, and the integrative theory of law understanding avoids current problems in the field of law enforcement and judicial practices emerging in the digital environment. Also, an attempt was made to formulate special principles for consumer legal relations that allow the most successful consideration of actual issues and disputes involving consumers as a result of their actions in the digital environment.

Keywords: Legal understanding, Digitalization, Integrative theory, Consumer legal relations, Justification of law, Consumer, Gaps in the law, Erroneous judicial practice, Digital environment

Изменение порядка совершения действий в торговом обороте и перевод многих процессов в цифровую форму, где технологии занимают одну из главенствующих ролей, наблюдается на повсеместной основе в различных сферах общественной жизни. Только за последние несколько лет в рамках правового и индивидуального регулирования сотни форм взаимоотношений либо уже были переведены в цифровую среду, либо были зафиксированы однозначно направленные шаги по их оцифровке: виртуальное пространство, киберпространство; онлайн-покупки и кредитование; информационно-посреднические платформы [1; 2. С. 166–125], владельцы агрегаторов и цифровое посредничество [5. С. 68–82]; брокерские и инвестиционные счета, доступные каждому с мобильного устройства, позволяющего в несколько мгновений становится участником корпоративных правоотношений; цифровые магазины без продавцов [4. С. 17–23]; виртуальные образовательные платформы; смарт-контракты [3. С. 35–41], криптовалюта и электронная торговля [6. С. 11–20] и другие аспекты цифровой жизни плотно внедрились в повседневную жизнь потребителей. Кроме того, государственные органы и организации также стараются делать шаги на пути к цифровизации. Так, в сфере государственных (муниципальных) закупок на территории ЕАЭС утверждается перечень мер для полноценной цифровизации (Распоряжение Коллегии ЕАЭС от 23.08.2022 № 140); службой финансового уполномоченного в Российской Федерации отмечается, что планируется к внедрению ряд цифровых новшеств применительно к порядку взаимодействия с потребителями финансовых услуг (электронные каналы общения, обработка через единый портал государственных услуг и т. д.) [12. С. 56–61]; Роспотребнадзором утверждены цели по цифровизации государственных услуг, связанных с созданием Единой информационно-аналитической системы Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека/ЕИАС Роспотребнадзора (Ведомственная программа цифровой трансформации Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека на 2021–2023 гг., утв. Роспотребнадзором); вопросы, связанные с цифровой прослеживаемостью, обсуждаются и внедряются на территории ЕАЭС и т. д.

Однако, несмотря на многие инициативы, а также изменения в области правового регулирования цифровых правоотношений, по-прежнему существуют пробелы в области нормативного регулирования фактически складывающихся отношений между субъектами права. В частности, на данное обстоятельство обращает свое внимание ЦБ РФ, который указывает, что, несмотря на все блага, которые предоставляет цифровая среда и диджитализированные продукты, защита потребителей финансового рынка от мошенничества и кибератак является одним из приоритетных направлений («Основные направления развития финансового рынка Российской Федерации на 2022 г. и период 2023 и 2024 гг.», утвержденные ЦБ РФ). В связи с чем и в условиях, когда технологические аспекты и предложения явным образом опережают законодательное урегулирование соответствующих отношений, вопрос о том, что является правом и неправом в условиях цифровизации, видится довольно актуальным, поскольку он имеет прямое отражение, в том числе на потребителях – лицах, как правило, не обладающих значительными знаниями в цифровых областях и их правовом регулировании, вместе с тем, как правило, жертвами мошенников являются именно последние.

Как отмечается, в юридической литературе исследование теорий о правопонимании: юридического позитивизма и других не утрачивает актуальности с течением времени [14. С. 9–18]. Как известно, позитивизм рассматривает право как явление, производное от правовых норм. Основоположником такой концепции является австро-американский ученый-юрист Г. Кельзен. Ученый полагал, что право относится к сфере долженствования, которая находится вне зависимости от действительности. Его точка зрения была такова, что право – это совокупность правил поведения, которые выражены в правовых актах государства и регулируют общественные отношения со стороны должного, независимого от реальной жизни [9]. Среди сторонников теории юридического позитивизма необходимо отметить Г. Ф. Шершеневича, по мнению которого право обладает следующими характеристиками: нормативность; определение отношения человека к человеку; выступает угрозой страдания в случае его нарушения; исходит от государства [16]. Как уже среди современников отмечается, что право – это правила, закрепленные в официальном государственном документе, которые носят общеобязательный характер и выполняются под страхом применения санкции в случае неповиновения [10. С. 51–59].

Однако, как отмечается в юридической литературе, цифровые технологии, помимо новых возможностей для реализации прав и законных интересов, также содержат угрозы для участников общественных отношений, связанные с вмешательством в их законные права и свободы [7. С. 15–17], которые не находят мгновенного отражения в системе правового регулирования, в связи с чем в целом ряде случаев усматривается, что общие теории правопонимания не способны в полной мере удовлетворить потребности чрезвычайно изменяющегося оборота. В этой связи весьма справедливым является замечание профессора В. М. Сырых, который указывает, что, как и любая правовая концепция, теория юридического позитивизма имеет ряд достоинств и недостатков. По его мнению, теория имеет ряд противоречий, не раскрывает закономерностей развития права и не дает научного определения понятию «право». Также В. М. Сырых полагает, что позитивное право не может быть единственной формой права. Среди недостатков данной теории также можно назвать отсутствие критериев, которые могли бы позволить отличить действительные правовые нормы от произвола власти; отсутствие возможности нравственной оценки правовых явлений; игнорирование естественных прав человека [13. С. 38–44]. Также слепое следование исключительно положениям закона может приводить в целом к выводу о том, что отношения являются нелегитимными, т. е. неспособными являться основанием для возникновения соответствующих правовых последствий у его участников. Такого рода подход нередко встречается в судебной практике, где суды, руководствуясь подходом «предусмотрено или не предусмотрено законом», принимают весьма неоднозначные или даже ошибочные решения. Схожие наблюдения делает А. И. Савельев, который указывает, что текущая действительность такова, что судебные органы руководствуются не принципами права, а исходят из формального текста закона и позиций регуляторов, нередко неофициального характера. Примеры такого подхода мы можем наблюдать в спорах, связанных с криптовалютами. Формально они не запрещены действующим законодательством, однако существующие рестриктивные позиции регуля-

торов, обусловленные публично-правовыми соображениями, находят отклик в судебных решениях [11. С. 60–92]. Аналогичная позиция усматривается в судебной практике. Так, в одном из дел суд указал: «Биткоин не подпадает под определение электронных денежных средств, которое дано в п. 18 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ "О национальной платежной системе", а также не подпадает под определение платежной системы, которое содержится в п. 20 ст. 3 этого же Закона, не является иностранной валютой (п. 2 ч. 1 ст. 1 Федерального закона от 10.12.2003 № 173-ФЗ "О валютном регулировании и валютном контроле"). В Российской Федерации отсутствует правовая база для регулирования платежей, осуществляемых в "виртуальной валюте", торговых интернет-площадок, биткоин-бирж, все операции с перечислением биткоинов производятся их владельцами на свой страх и риск…» (Постановление Десятого арбитражного апелляционного суда от 14.12.2020 № 10АП-16821/2020 по делу № А41–4212/2020). В свете данных событий, например, Т. Я. Хабриева и Н. Н. Черногор отмечают, что правовая наука столкнулась с необходимостью выполнения определенных фундаментальных задач, среди которых разработка юридического инструментария, связанного с регулированием вопросов виртуального и реального права, а также общественных отношений, связанных с использованием и применением в повседневной жизни цифровых технологий [15. С. 85–102].

Обозначенные проблемы в теории права, в правоприменительной и судебной практике, демонстрирующей существование пробелов, а также утверждения о предстоящих фундаментальных задачах в области права указывают на существование действительной проблемы в сфере правопонимания. Вместе с тем представляется, что ситуация выглядит несколько иначе. Полагаем, что в существующих реалиях, связанных с цифровизацией общественных отношений, в том числе в сфере потребительских правоотношений как наиболее уязвимой категории, а также явно неразработанной нормативно-правовой базы в сфере регулирования отношений, возникающих в цифровой среде и с использованием соответствующих технологий, концепция интегративного правопонимания является наиболее оправданной с точки зрения науки, которая, как представляется, не допускает «слепого» подхода к рассмотрению вопроса путем утверждения о том, предусмотрено то или иное положение законом или нет. Ведь одним из значимых преимуществ указанной концепции является то обстоятельство, что право в большинстве случаев беспробельно, поскольку не ограничивается только нормами права, содержащимися в «законодательстве» [8. С. 36–39]. Один из основоположников теории интегративного правопонимания В. В. Ершов обоснованно утверждает, что с позиции интегративного правопонимания право выражается в принципах и нормах права, поэтому пробел в праве (а не в законодательстве), на взгляд профессора, теоретически возможен только при отсутствии принципов и норм права во всех формах как внутригосударственного, так и международного права, реализуемых в России [8. С. 39–42], что, как очевидно, не является релевантным для существующей системы права. Следовательно, в условиях цифровизации, т. е. появления новых объектов, субъектов, способов взаимодействия и выстраивания правоотношений между ее участниками, позиция правоприменительных и судебных органов,

а также иных концептуальных правовых теорий, согласно которым не предусмотренные законом положения не должны признаваться легитимными в обороте, являются несостоятельными; а теория интегративного правопонимания как в целом, так и применительно к вопросам цифровизации должна заслуживать всяческой поддержки, поскольку благодаря ее фундаментальному подходу о том, что отношения, прежде всего, должны регулироваться на основании установленных принципов права, пробелов в регулировании фактически складывающихся отношений не должно возникать в целом, поскольку основополагающие (общие) и специальные принципы права, являющиеся самостоятельными средствами правового регулирования общественных отношений, применяются непосредственно, а не по «аналогии права» [8. С. 43–44]; таким образом, проблема с пробелами в праве, в том числе в условиях цифровизации, является решенной, так как они в целом отсутствуют.

При данных обстоятельствах, руководствуясь интегративным подходом правопонимания и принимая во внимание чрезвычайно развивающиеся потребительские отношения в условиях цифровизации, представляется допустимым выдвинуть следующие специальные принципы, через призму которых необходимо регулировать и разрешать фактически возникающие спорные вопросы в сфере потребительских отношений, в том числе возникающие с использованием современных технологий и цифровой среды, если иное не будет доказано:

I. Если потребитель смог разобраться с порядком использования цифровых технологий, чтобы вступить в отношения в цифровой среде, значит, он имел возможность и/или должен был изучить соответствующие особенности порядка взаимодействия и характеристики приобретаемого/отчуждаемого объекта, которые доводятся до его сведения и раскрываются явным, т. е. нескрытым, образом.

II. В случае вступления потребителя в отношения по поводу приобретения/отчуждения объекта в цифровой среде он выражает, прежде всего, согласие со следующими аспектами:

1) какое благо потребитель выбрал;

2) какую цену должен уплатить потребитель за соответствующее благо;

3) что он ознакомлен с прямо (без дополнительных переадресаций в сети Интернет или указанием о возможности ознакомления) предоставленным ему материалом и условиями в процессе совершения им конклюдентных действий на пути совершения цифровой сделки, т. е. на пути прослеживаемого цифрового следа потребителя;

4) что к нему и его данным будут относиться справедливо, разумно и в необходимых для совершения цифровой сделки пределах.

Указанные специальные принципы совместно с интегративной теорией правопонимания позволят, как представляется, наиболее успешно защищать интересы права и законные интересы потребителей, а также обязывать последних задумываться и принимать взвешенные решения, в том числе по поводу приобретения «новых» и еще не полностью известных объектов, поскольку первооткрывателей всегда сопровождает как возможность приобретения существенного блага, так и риск полной потери.

Выводы. Теория интегративного правопонимания позволяет на эффективной основе регулировать фактически складывающиеся отношения между их участни-

ками независимо от среды их возникновения, в том числе в условиях цифровизации бытия.

Потребительские отношения, возникающие в цифровой среде, необходимо рассматривать через призму интегративного правопонимания с учетом специальных принципов, которые сводятся к следующему:

– если потребитель смог разобраться с порядком использования цифровых технологий, чтобы вступить в отношения в цифровой среде, значит, он имел возможность и/или должен был изучить соответствующие особенности порядка взаимодействия и характеристики приобретаемого/отчуждаемого объекта, которые доводятся до его сведения и раскрываются явным, т. е. нескрытым, образом;

– в случае вступления потребителем в отношения по поводу приобретения/отчуждения объекта в цифровой среде он выражает, прежде всего, согласие со следующими аспектами:

1) какое благо потребитель выбрал;

2) какую цену должен уплатить потребитель за соответствующее благо;

3) что он ознакомлен с прямо (без дополнительных переадресаций в сети Интернет или указанием о возможности ознакомления) предоставленным ему материалом и условиями в процессе совершения им конклюдентных действий на пути совершения цифровой сделки, т. е. на пути прослеживаемого цифрового следа потребителя;

4) что к нему и его данным будут относиться справедливо, разумно и в необходимых для совершения цифровой сделки пределах.

Список литературы

1. Белов В. А. Комментарий к проекту Директивы Европейского союза «Об онлайн-посреднических платформах» с переводом. – Москва: М-Логос, 2022. 68 с.

2. Белов В. А. Онлайн-посреднические платформы: обсуждаемые подходы и отечественная система правового регулирования // Закон. 2022. № 6. С. 116–125.

3. Белов В. А. Смарт-контракт: понятие, правовое регулирование, правоприменительная практика, потребительские отношения // Право и экономика. 2021. № 9 (403). С. 35–41.

4. Белов В. А. Смарт-торговля (цифровая торговля): основные положения о цифровизации договорных отношений с участием потребителей // Вестник арбитражной практики. 2022. № 3 (100). С. 17–23.

5. Белов В. А. Цифровое посредничество и потребительские отношения: правовая природа и ответственность // Актуальные проблемы российского права. 2022. Т. 17, № 8 (141). С. 68–82.

6. Белов В. А. Электронная торговля: понятие, правовое регулирование и судебная практика // Вестник арбитражной практики. 2021. № 4 (95). С. 11–20.

7. Гончаров И. В. Конституционные ценности в эпоху «цифровых технологий» // Конституционное и муниципальное право. 2019. № 11. С. 15–17.

8. Ершов В. В. Пробелы в национальном и международном праве с позиций юридического позитивизма, синтезированного и интегративного правопонимания // Российское правосудие. 2017. № 2. С. 36–44.

9. Кельзен Г. Чистое учение о праве. 1960 / пер. с нем. М. В. Антонова, С. В. Лезова. Санкт-Петербург: Издательский дом «Алеф-Пресс», 2015. 542 с.

10. Колосов И. В. Юридический позитивизм Джона Остина и утилитаризм Иеремия Бентама: диалектика соотношения // Вопросы российского и международного права, 2017. Том 7. № 3А. С. 51–59.

11. Савельев А. И. Гражданско-правовые аспекты регулирования оборота данных в условиях попыток формирования цифровой экономики // Вестник гражданского права. 2020. № 1. С. 60–92.

12. Служба усилит свое влияние на поведение финансовых организаций // Современные страховые технологии. 2021. № 3. С. 56–61.

13. Сырых В. М. Застарелые недуги позитивистской доктрины права // Право и государство. 2014. № 2. С. 38–44.

14. Тарасов Н. Н. Юридический позитивизм и позитивистская юриспруденция (Апология догмы права) // Российский юридический журнал. 2016. № 6. С. 9–18.

15. Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85–102.

16. Шершеневич Г. Ф. Общая теория права. II выпуск. Москва: Издательство бр. Башмаковых, 1910. 698 с.

А. Ю. Бурова,
преподаватель,
Нижегородский государственный университет имени Н. И. Лобачевского

ОБЗОР РОССИЙСКОГО РЫНКА ОПЕРАТОРОВ ИНВЕСТИЦИОННЫХ ПЛАТФОРМ

Аннотация. В настоящей статье исследуется развитие российского рынка операторов инвестиционных платформ. По результатам анализа реестра операторов инвестиционных платформ, официальных сайтов и правил существующих инвестиционных платформ демонстрируется рост количества операторов инвестиционных платформ, устанавливаются преобладающие способы инвестирования, выявляется взаимосвязь способа инвестирования и статуса оператора инвестиционной платформы на рынке ценных бумаг. Автором демонстрируется разнообразие сфер осуществления деятельности операторов инвестиционных платформ по организации привлечения инвестиций.

Ключевые слова: оператор инвестиционной платформы, инвестиционная платформа, содействие инвестированию, привлечение инвестиций, способы инвестирования

SURVEY OF RUSSIAN MARKET OF INVESTMENT PLATFORM OPERATORS

Abstract. The article examines the development of the Russian market of investment platform operators. Based on the results of the analysis of the register of investment platform

operators, official internet sites and rules of existent investment platforms growth of number of investment platform operators is demonstrated, prevailing investment methods are stated, correlation between investment method and status of investment platform operator on the security market is revealed. The author demonstrates the variety of spheres of investment platform operators` activity on facilitating the investment.

Keywords: Investment platform operator, Investment platform, Facilitating the investment, Attraction of investments, Investment methods

Введение. С 1 января 2020 г. вступил в силу Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Закон об инвестиционных платформах) [4]. Указанный закон регламентирует правовые основы статуса новых субъектов предпринимательской деятельности – операторов инвестиционных платформ (далее – ОИП), которые осуществляют деятельность по организации привлечения инвестиций с использованием онлайн посреднической информационной системы (инвестиционной платформы).

Как представляется, изучению особенностей правового регулирования деятельности ОИП и поиску адекватных правовых механизмов опосредования такой деятельности и защиты прав инвесторов и заемщиков должно предшествовать детальное исследование разнообразия функционирующих в России ОИП, поскольку именно разнообразие способов и направлений инвестирования, а также сочетание функций ОИП с функциями других субъектов предпринимательской деятельности должны обуславливать специфику регулирования деятельности ОИП. По прошествии двух с половиной лет можно сделать определенные выводы относительно популярности инвестирования на онлайн платформах, преобладания того или иного способа инвестирования, разнообразия сфер инвестирования.

Основная часть. В соответствии с понятием оператора инвестиционной платформы, зафиксированного в пп. 7 п. 1 ст. 2 Закона об инвестиционных платформах, ОИП включается Банком России в реестр операторов инвестиционных платформ. Данный реестр выполняет правоустанавливающую функцию, так как без внесения оператора в соответствующий реестр его деятельность по организации привлечения инвестиций невозможна. При этом следует отметить, что ранее краудфандинг в России законодательного регулирования не имел, поэтому некоторые платформы действовали на основании разработанных ими самими правил пользования платформой и типовыми формами договоров с пользователями. В настоящее время данные платформы были вынуждены привести свое внутреннее регулирование в соответствие с требованиями закона об инвестиционных платформах, который частично предопределяет содержание правил, а также приобрести статус ОИП путем регистрации в соответствующем реестре.

По состоянию на 29 июля 2022 г. в реестр ОИП включены 63 оператора. [7]. При этом количество операторов стабильно увеличивается (график 1), а два оператора уже были исключены из реестра.

Согласно результатам исследований, проведенных зарубежными учеными, к факторам, влияющим на намерение людей использовать инвестиционные онлайн-платформы, относятся как минимум удобство в использовании (ease of use), безопасность (security), финансовый результат (financial return) [8. P. 169]. Представляется, что перечисленные факторы вполне могут обуславливать распространение онлайн-инвестирования с помощью инвестиционных платформ и ежегодного роста включаемых в реестр Банка России ОИП.

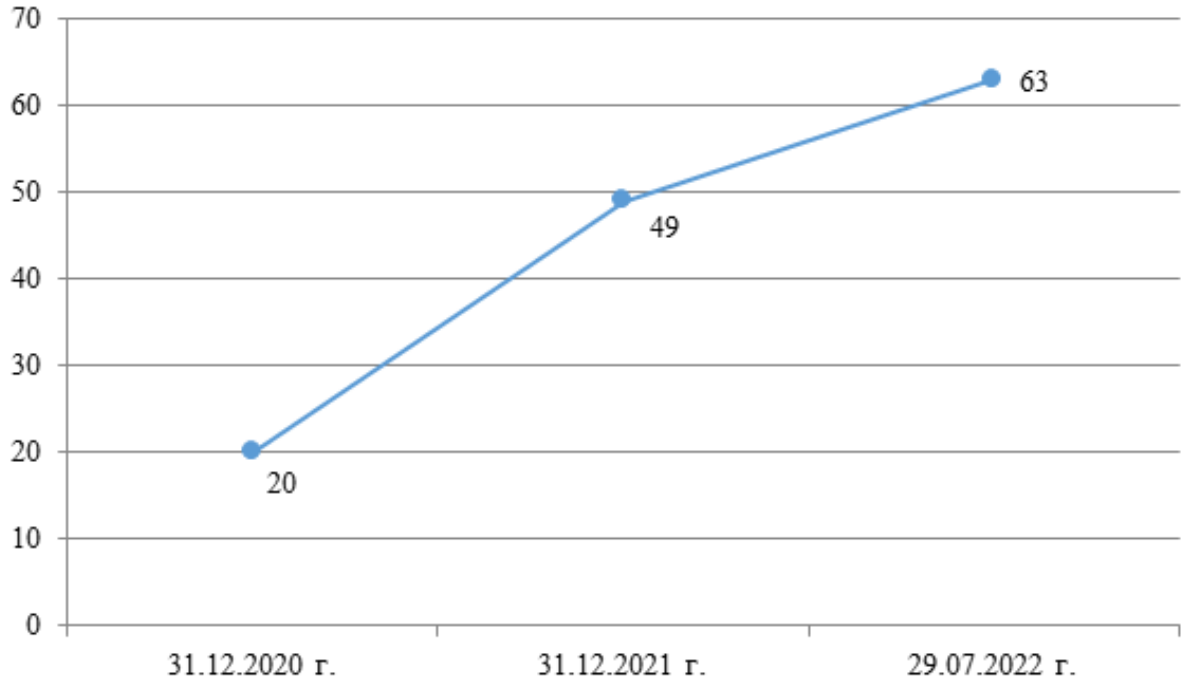

График 1. Рост количества операторов инвестиционных платформ

В целях развития различных краудфандинговых инструментов и расширения взаимодействия ОИП с другими субъектами предпринимательской деятельности и органами власти в Российской Федерации создана Ассоциация операторов инвестиционных платформ (далее – Ассоциация), предполагающая объединение операторов [6]. Из шестидесяти трех существующих в настоящее время в России ОИП Ассоциация на сегодняшний день объединяет лишь одиннадцать из них, что составляет менее 1/5 части всех существующих в России ОИП. Следовательно, пока преждевременно говорить о том, что Ассоциация является представителем интересов всего рынка российских ОИП.

В связи с тем, что ОИП содействуют в инвестировании инвесторам и оказывают услуги по привлечению инвестиций заемщикам К. В. Кванина и А. В. Спиридонова справедливо указывают, что основной функцией ОИП является организационно-посредническая. [3] А. В. Габов и И. В. Хаванова также называют ОИП посредником, обеспечивающим «функционирование инфраструктуры, на базе которой осуществляется инвестиционный процесс». [2. С. 39] В ст. 5 Закона об инвестиционных платформах выделяются четыре способа инвестиро-

вания с использованием инвестиционной платформы: путем предоставления займов; путем приобретения эмиссионных ценных бумаг, размещаемых с использованием инвестиционной платформы; путем приобретения утилитарных цифровых прав; путем приобретения цифровых финансовых активов.

Конкретные способы инвестирования на каждой инвестиционной платформе определяются разрабатываемыми ими документами. При этом большое значение Закон об инвестиционных платформах придает правилам инвестиционной платформы, которые содержат в основном частноправовое регулирование отношений, возникающих в связи с привлечением инвестиций с помощью инвестиционных платформ, и которые, по мнению В. К. Андреева, представляют собой «примерные условия договора (ст. 427 ГК РФ) и должны утверждаться на общем собрании участников (акционеров) общества как внутренние документы юридического лица (п. 5 ст. 52 ГК РФ)» [1]. Анализ правил шестидесяти существующих в России инвестиционных платформ1 позволяет сделать выводы относительно наиболее распространенных способов инвестирования (диаграмма 1).

Диаграмма 1

Как следует из проведенного анализа, результаты которого отражены выше, преобладающим способом инвестирования, который предлагается ОИП, является предоставление займов (45 инвестиционных платформ ограничивают свою деятельность только данным способом, еще 5 платформ осуществляют ее наряду с другими способами инвестирования). По нашему мнению, подобные количественные показатели также могут свидетельствовать о предоставлении займов

[1] Официальные сайты трех российских ОИП (АО «Инвестиционная платформа Крым», ООО «Народная инвестиционная платформа», ООО «Удалтон инвестиции») оказались недоступными.

как наиболее привычном и понятном для оформления и регулирования способе инвестирования, в отличие от новых и пока еще не так хорошо изученных иных способов, предлагаемых Законом об инвестиционных платформах. Так, ни один ОИП в настоящее время не предлагает инвестировать путем приобретения цифровых финансовых активов, и только две платформы (АО «СРК» и АО «СТАТУС») осуществляют деятельность по организации инвестирования путем приобретения утилитарных цифровых прав.

Содействие инвестированию путем приобретения эмиссионных ценных бумаг (как правило, акций непубличных акционерных обществ) осуществляется как компаниями, являющимися держателями реестра владельцев ценных бумаг (регистраторами) в соответствии с законодательством РФ о рынке ценных бумаг [5], так и компаниями, не являющимися регистраторами (диаграмма 2).

Диаграмма 2

Очевидно, что привлечение инвестиций путем реализации эмиссионных ценных бумаг с использованием инвестиционной платформы, оператор которой одновременно является регистратором, удобно для эмитента. В этом случае в рамках единого окна осуществляется и регистрация выпуска акций, и их последующее размещение на платформе.

Анализ официальных сайтов ОИП также приводит к выводу о том, что отдельные ОИП специализируются на содействии в инвестировании в узких отраслях. Например, существуют ОИП, организующие инвестирование в творческие проекты (ООО «Ко-Фи»), для исполнения государственных контрактов (ООО «МодульДеньги»), в коммерческую или жилую недвижимость (ООО «СИМПЛ ЭСТЭЙТ» и ООО «Кредит.Клаб» соответственно), в грузоперевозки (ООО «ЛЭНДЭР-ИНВЕСТ»), в различные проекты в сфере недвижимости (ООО «ТаланИнвест»). Представляется, что деятельность ОИП в столь различных сферах привлечения инвестиций должна повлечь за собой специфику в ее организации и использование специальных механизмов защиты прав инвесторов и заемщиков.

Выводы. Исследование российского рынка ОИП позволило сделать несколько важных, имеющих значение для дальнейших исследований выводов. В течение двух с половиной лет наблюдается устойчивый рост количества операторов инвестиционных платформ. В настоящее время в России существуют 63 ОИП. Созданная Ассоциация ОИП объединяет 11 из них, поэтому пока преждевременно говорить о том, что Ассоциация является представителем интересов всего рынка российских ОИП.

Преобладающим способом инвестирования с помощью инвестиционных платформ является предоставление займов, что объясняется относительной простотой оформления и привычностью использования такого инвестиционного инструмента. Ни один ОИП в настоящее время не предлагает инвестировать путем приобретения цифровых финансовых активов. Инвестирование путем приобретения эмиссионных ценных бумаг становится популярным у держателей реестров владельцев ценных бумаг, поскольку позволяет эмитентам зарегистрировать выпуск акций и разместить их для приобретения у одного и того же лица.

Некоторые ОИП специализируются на содействии в инвестировании в узких отраслях, что должно обуславливать специфику в его организации и использование специальных механизмов защиты прав инвесторов и заемщиков.

Список литературы

1. Андреев В. К. Договоры инвестирования, заключаемые с использованием инвестиционных платформ путем приобретения утилитарных цифровых прав // Юрист. 2020. № 1. С. 15–21.

2. Габов А. В., Хаванова И. А. Краудфандинг: законодательное оформление web-модели финансирования в контексте правовой доктрины и зарубежного опыта // Вестник Пермского университета. Юридические науки. 2020. № 1. С. 28–44.

3. Кванина В. В., Спиридонова А. В. Публично-правовое и частноправовое регулирование деятельности оператора инвестиционной платформы // Право и цифровая экономика. 2020. № 4. С. 25–31.

4. О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) // СЗ РФ. 2019. № 31. Ст. 4418.

5. О рынке ценных бумаг: Федеральный закон от 22.04.1996 № 39-ФЗ (ред. от 14.07.2022) // СЗ РФ. 1996. № 17. Ст. 1918.

6. Официальный сайт Ассоциации операторов инвестиционных платформ. URL: https://rus-crowd.ru/ (дата обращения: 02.08.2022).

7. Реестр операторов инвестиционных платформ. URL: https://cbr.ru/registries (дата обращения: 02.08.2022).

8. Gazali H. M., Adeyemi A. A., Alhabshi S. M. S. J. Exploring the Influential Factors on Online Investment Platform // Materials of 6th International Conference on Information and Communication Technology for the Muslim World. 2016. Pp. 166–170.

Н. Г. Вилкова,
заслуженный юрист Российской Федерации,
доктор юридических наук, профессор, профессор кафедры
международного частного права,
Всероссийская академия
внешней торговли Министерства экономического развития
Российской Федерации,
член Президиума Международного коммерческого арбитражного суда
при Торгово-промышленной палате Российской Федерации

ЦИФРОВЫЕ ТЕХНОЛОГИИ И МЕЖДУНАРОДНЫЙ АРБИТРАЖ

Аннотация. В статье рассматриваются вопросы развития цифровизации разбирательства споров в международном коммерческом арбитраже на примере ведущих арбитражных центров: Арбитражного суда Международной торговой палаты (ICC), Международного коммерческого арбитражного суда при Торгово-промышленной палате России. Выделяются документы, принятые этими арбитражными центрами для обеспечения онлайн-слушаний, представления документов, опроса свидетелей и экспертов. Отдельно рассматривается рекомендательный документ 2022 г. Инструментарий стандартов для трансграничной безбумажной торговли, разработанный ICC и Всемирной торговой организацией (WTO). Выделяется роль Комиссии ООН по праву международной торговли (ЮНСИТРАЛ), которой начиная с 1987 г. подготовлен юридический фундамент для реализации цифровизации арбитражного разрешения споров.

Ключевые слова: международный арбитраж, цифровизация, трансграничные споры, конвенции, типовые законы, безбумажная торговля

DIGITAL TECHNOLOGIES AND INTERNATIONAL ARBITRATION

Abstract. The article discusses the development of digitalization of dispute resolution in international commercial arbitration on the example of the leading arbitration centers: the Court of Arbitration of the International Chamber of Commerce (ICC), the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry. Documents accepted by these arbitration centers to ensure online hearings, submission of documents, interviews of witnesses and experts are highlighted. The 2022 advisory document, the Standards Toolkit for Cross-border Paperless Trade, developed by the ICC and the World Trade Organization (WTO), is considered separately. The role of the UN Commission on International Trade Law (UNCITRAL), which, since 1987, has prepared the legal foundation for the implementation of the digitalization of arbitration dispute resolution, is highlighted.

Keywords: International arbitration, Digitalization, Cross-border disputes, Conventions, Model laws, Paperless trade

Учитывая, что международный арбитраж является наиболее востребованным способом разрешения споров из транснациональных контрактов, развитие

цифровых технологий для быстрого и справедливого разрешения споров имеет важное значение. Во-первых, это необходимо для оформления контрактов и сопроводительной документации, претензионной переписки в цифровой форме; во-вторых, это связано с порядком разрешения споров из указанных контрактов международными арбитражами.

Цифровизация в международном коммерческом арбитраже, который рассматривает большинство споров между хозяйствующими субъектами различных государств, а также между российскими юридическими лицами является весьма актуальной проблемой. Это связано с рядом факторов: значительное число обращений фирм, компаний и предприятий в международный арбитраж, возникших в связи с пандемией COVID-19, сложности с перемещением сторон и арбитров, а действующие начиная с 2014 г. санкции со стороны недружественных государств, и особенно в современный период, породили два вида проблем: арбитражное разбирательство споров и исполнение арбитражных решений в стране ответчика.

Статистика Международного коммерческого арбитражного суда при ТПП РФ за 2021 г. [1], приведенная на рис. 1, свидетельствует о значении деятельности данного всемирно признанного центра международного арбитража в современный период.

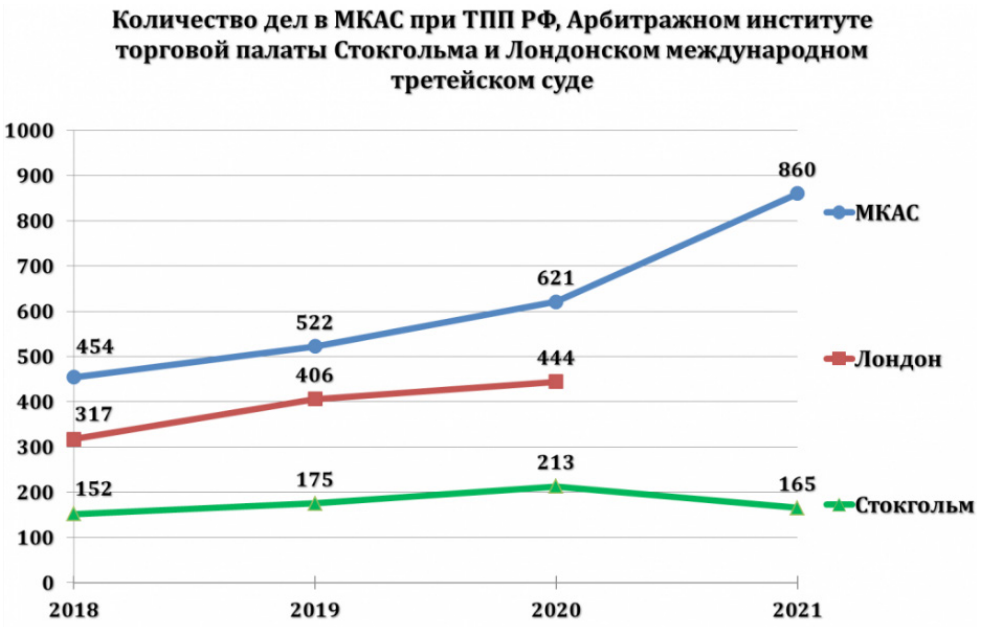

Рис. 1. Статистика МКАС при ТПП РФ за 2021 г.

На совещании с руководителями региональных палат, с участием которых образованы отделения Международного коммерческого арбитражного суда (МКАС) и Морской арбитражной комиссии (МАК) президент Торгово-промышленной палаты РФ С. Н. Катырин 15 декабря 2021 г. отметил, что образовано 22 отделения МКАС и отделение МАК в Санкт-Петербурге. Он подчеркнул, что в 2021 г. безусловным лидером по количеству дел стало отделение МКАС в Казани (79 дел) [2]. На рис. 2 показано количество внутренних споров в отделениях МКАС в период 2017–2021 гг.

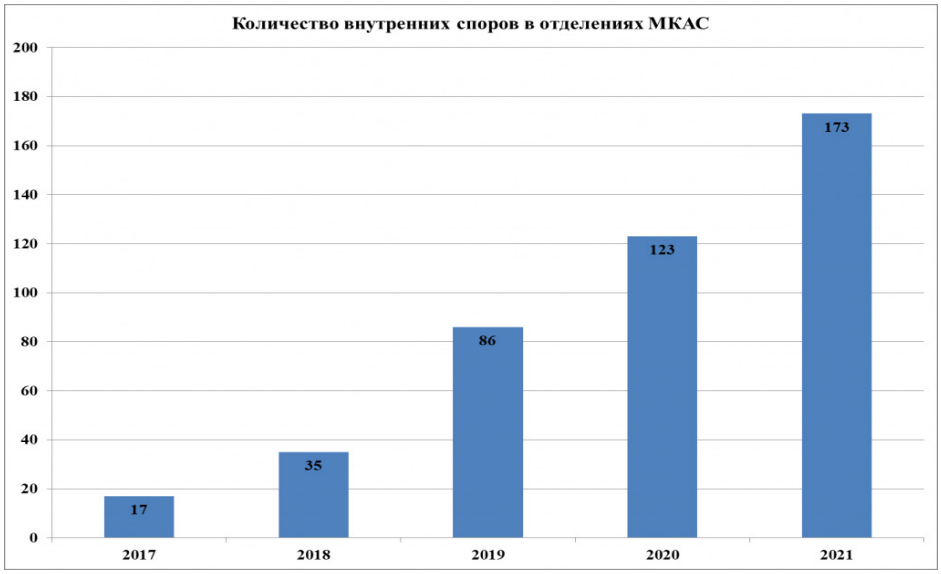

Рис. 2. Количество внутренних споров в отделениях МКАС 2017–2021 гг.

Обращение к статистике наиболее известного Международного Арбитражного суда при Международной торговой палате (ICC International Court of Arbitration) показывает, что в 2021 г. Секретариат Международного арбитражного суда ICC зарегистрировал в общей сложности 853 новых дела, в том числе 840 дел, поданных в соответствии с Арбитражным регламентом ICC, вступившим в силу с 1 января 2021 г. В новых делах в 2021 г. участвовало 2206 сторон из 143 стран (первые пять мест заняли стороны из США, Бразилии, Испании, Объединенных Арабских Эмиратов и Мексики, в первую десятку вошли стороны из Франции, Германии, КНР и Специального административного района Гонконг, Индии и Италии). С участием российских сторон ежегодно рассматривается примерно 25–30 споров. Сумма передаваемых в арбитраж споров колеблется от 9500 долл. США до более 27 миллиардов долл. США.

Основная роль в создании юридических основ правового регулирования цифровизации коммерческого оборота принадлежит Комиссии ООН по праву международной торговли (ЮНСИТРАЛ). Данная работа была начата в 1987 г. с принятием Правового руководства по переводу средств [3], в котором рассматриваются правовые вопросы, возникающие при переводах денежных сумм с использованием электронных средств. Затем в 1996 г. ЮНСИТРАЛ приняла Типовой закон об электронной торговле [4]. О значимости этого документа свидетельствует тот факт, что на основе или под влиянием этого Типового закона приняты соответствующие законы в 164 юрисдикциях в 83 государствах. Он основан на установлении функционального эквивалента для концепций коммуникаций, использующих бумажный документооборот (письменная форма, подпись и оригинал), и содержит стандарты, по которым может оцениваться правовое значение электронных сообщений для расширения использования безбумажных способов коммуникации.

ЮНСИТРАЛ в 2001 г. принят Типовой закон об электронных подписях [5] (на его основе национальные законы приняты в 39 юрисдикциях в 38 государствах),

а в 2005 г. принята Конвенция об использовании электронных сообщений в международных договорах [6] (контрактах). Конвенция вступила в силу 1 марта 2013 г., в ней участвуют 16 стран, включая Российскую Федерацию. Конвенция применяется ко всем электронным сообщениям, являющимся предметом обмена между сторонами, коммерческие предприятия которых находятся в разных государствах, если коммерческое предприятие хотя бы одной стороны находится в договаривающемся государстве (ст. 1). Она также может применяться на основании выбора сторон договора.

В Конвенции определены критерии для установления функциональной эквивалентности между электронными сообщениями и бумажными носителями и между электронными методами удостоверения подлинности и собственноручных подписей. Важными являются положения Конвенции (ст. 8) о том, что сообщения не могут быть лишены юридической силы только потому, что они составлены в электронной форме; также признается исковая сила договоров, заключенных с помощью автоматизированных систем сообщений, в том числе в случаях, когда никакое физическое лицо не осуществляло просмотра выполненных ими отдельных операций (ст. 12).

В 2017 г. ЮНСИТРАЛ принят **Типовой закон об электронных передаваемых записях** [7], на его основании приняты национальные законы в семи государствах. Особое значение имеет положение Типового закона о его применении к электронным передаваемым записям, которые являются функциональными эквивалентами оборотных документов или инструментов. В случаях, когда законодательство требует, чтобы информация была представлена в письменной форме, это требование считается выполненным в отношении электронной передаваемой записи, если содержащаяся в ней информация является доступной для последующего использования.

Таким образом, ЮНСИТРАЛ создан юридический фундамент, обеспечивающий цифровизацию транснационального коммерческого оборота, от заключения договора, обмена соответствующими документами, осуществления платежей и т. д.

Значительная работа, направленная на цифровизацию транснационального коммерческого оборота, проводится Международной торговой палатой (ICC). Следует выделить деятельность Комиссии ICC по коммерческому праву и практике, которой традиционно разрабатывается рекомендательный документ, признанный по всему миру обычаем делового оборота – Инкотермс. Понимая значимость электронного оформления и оборота документов, сопровождающих исполнение контракта международной купли-продажи, разработчики этого документа впервые в Инкотермс 2000 включили в пп. А1 и А8 всех терминов следующее упоминание об электронных сообщениях: Инкотермс 2000: согласно п. А1 всех терминов, продавец обязан поставить товар в соответствии с договором купли-продажи и представить коммерческий счет-инвойс или эквивалентное ему электронное сообщение, а также любые иные доказательства соответствия товара, которые могут потребоваться по условиям договора. Согласно п. А8, продавец обязан предоставить покупателю за свой счет в качестве доказательства поставки обычные транспортные документы в соответствии с пунктом А4… В случае если продавец и покупатель договорились об использовании средств электронной связи, упомянутые документы могут быть заменены эквивалентными им электронными сообщениями (EDI). Согласно п. Б8 покупатель обязан принять доказательства поставки в соответствии с п. А8.

Расширение возможности использовать безбумажный обмен документами предусматривалось в Инкотермс 2010: согласно п. А1/Б1 всех терминов любой документ, упомянутый в пп. А1–А10/Б1–Б10, может быть в виде эквивалентной электронной записи или иной процедуры, если это согласовано сторонами или является обычным. Согласно Инкотермс 2020: согласно п. А1/Б1, любой документ, представленный продавцом/покупателем, может быть в бумажной или электронной форме, если это согласовано, а при отсутствии соглашения – в соответствии с обычаями делового оборота.

За двадцать лет от согласования продавцом и покупателем представление документов использования средств электронной связи и замене бумажных документов эквивалентными им электронными сообщениями (EDI) изменилось на возможность каждой стороны представить любой документ в бумажной или электронной форме, если это согласовано, а при отсутствии соглашения – в соответствии с обычаями делового оборота. Учитывая, что, согласно в ст. 5 Гражданского кодекса Российской Федерации (ГК РФ), обычай признан нормативным регулятором отношений, регулируемых кодексом, продавцу и покупателю необходимы знания об обычаях делового оборота, действующих в сфере обмена документами в коммерческом обороте.

Глобальная торговля, оцениваемая в 28 триллионов долл. США, является основой мировой экономики. Тем не менее торговля через границы – это заведомо сложный процесс, который в значительной степени зависит от бумажных документов, несмотря на многолетние усилия по цифровизации. Трансграничная сделка включает в себя несколько участников и в среднем требуется обмен 36 документами и 240 копиями, однако в настоящее время менее одного процента торговых документов полностью оцифровано [8].

Для ознакомления участников торговых операций с возможностями цифровизации документов ICC и ВТО в 2022 г. разработан Инструментарий стандартов для трансграничной безбумажной торговли [8], направленный на ускорение цифровизации посредством использования стандартов, которые известны всем коммерсантам (например, стандарты ISO). В этой рекомендации «стандарт данных» относится к стандартам, которые определяют основные элементы электронной записи, представляющей этот конкретный торговый документ, а «стандарт формата данных/обмена данными» относится к стандартам, которые помогают облегчить обмен данными между различными системами, принадлежащими разным участникам цепочки поставок. Документ включает шесть разделов, включающих, помимо указанных стандартов, рекомендации корпорациям и микро-, малым и средним предприятиям; перевозчикам, экспедиторам и логистическим операторам; таможенным органам и другим трансграничным регулирующим органам.

Пользователям предлагаются наиболее часто используемые стандарты для оцифровки потока часто используемых документов на каждом этапе «покупка – доставка – оплата». Например, стандарт 3.1 предлагает пользователям необходимые данные для документов, оформляющих коммерческие транзакции при покупке (buy process), стандарт 3.2 – необходимые данные, необходимые экспедиторам для доставки товаров (ship process), стандарт 3.3 – информация, необходимая для

оплаты товара, стандарт 3.4 – информация, касающаяся таможенного оформления и прохождения товара через границу. Правила данного документа обобщают современные способы автоматического обмена структурированными документами между продавцом и покупателем в электронном формате без ручного вмешательства.

Таким образом, в процессе разрешения спора стороны могут представлять электронные документы.

Вторая важная составляющая разрешения споров международным арбитражем затрагивает процесс разрешения споров: представление документов, проведение арбитражного разбирательства, участие представителей сторон и свидетелей, вынесение решения. Данные вопросы регулируются регламентами тех арбитражных центров, в которые стороны своим арбитражным соглашением согласились передать свои споры. Как указано в п. 12 ФЗ № 382 Федерального закона об арбитраже 2015 г. в действующей редакции, правила арбитража, на которые ссылается арбитражное соглашение, рассматриваются в качестве неотъемлемой части арбитражного соглашения [9].

Вопросам цифровизации третейского разбирательства споров из транснациональных контрактов действующее российское законодательство уделяет значительное внимание. Так, согласно п. 4 ст. 7 Закона о МКА 1993 г. в действующей редакции [10] арбитражное соглашение считается заключенным в письменной форме в виде электронного сообщения, если содержащаяся в нем информация является доступной для последующего использования и если арбитражное соглашение заключено в соответствии с требованиями закона, предусмотренными для договора, заключаемого путем обмена документами посредством электронной связи.

Использование систем видео-конференц-связи предусмотрено п. 1 § 27, п. 6 § 30 Правил арбитража международных коммерческих споров (Правил арбитража международных коммерческих споров) и п. 4 § 22 Правил арбитража внутренних споров. Президиумом МКАС одобрена новая формулировка данных правил: при необходимости по просьбе стороны или по собственной инициативе третейский суд, запросив мнение сторон, вправе с учетом обстоятельств дела и наличия технических возможностей провести устное слушание для заслушивания свидетелей, экспертов или сторон с использованием систем видео-конференц-связи или иных подходящих средств связи. При этом участие в таком устном слушании возможно как с личным присутствием, так и дистанционно с нахождением арбитров и других участвующих в устном слушании лиц в разных местах. Секретариатом МКАС разработаны правила организации слушаний онлайн для сторон.

Еще в 2017 г. Комиссией ICC по арбитражу и ADR подготовлен отчет «Информационные технологии в международном арбитраже» в виде обновленного обзора вопросов, которые следует учитывать при использовании информационных технологий в международном арбитраже [11]. Документ содержит десять разделов, затрагивающих вопросы цифровизации на отдельных стадиях арбитражного разбирательства: 1) согласие на использование IT в соглашении об арбитраже, после возникновения спора, 2) IT и выбор арбитров, 3) арбитражное разбирательство:

роль сторон, роль состава арбитров, проблемы совместимости, электронный обмен доказательствами, представление позиции, проблемы целостности данных, доказательство обслуживания, конфиденциальность и безопасность данных, интеллектуальная собственность, 4) слушание дела. В Приложении приведены примеры формулировок, которые можно использовать для использования IT.

12-й Обзор международного арбитража 2021 г., проведенный Queen Mary University in London и международной юридической фирмой White & Case «Адаптация арбитража к изменяющемуся миру» [12], подтверждает, что международный арбитраж является предпочтительным методом разрешения трансграничных споров для 90 % респондентов либо самостоятельно (31 %), либо в сочетании с ADR (59 %). Увеличение использования виртуальных залов для слушаний, по-видимому, является результатом того, как практика арбитража адаптировалась к пандемии COVID-19, поскольку пользователи были вынуждены искать альтернативы очным слушаниям. Если бы слушание больше не могло проводиться лично, 79 % респондентов предпочли бы «продолжить слушание в назначенное время в виде виртуального слушания». Только 16 % «отложили бы слушание до тех пор, пока оно не может быть проведено лично», а 4 % предпочли бы учитывать только документы. Аспекты, которые вызывали у респондентов наибольшие опасения, включали «трудности приспосабливания к нескольким или разным часовым поясам», впечатление, что «группам консультантов и клиентам труднее совещаться во время слушаний», а также опасения, что это может быть труднее контролировать свидетелей и оценить их достоверность. Также упоминались ошибочность технологий и явление «усталости экрана».

После пандемии респонденты предпочли бы «сочетание личного и виртуального» форматов практически для всех видов взаимодействия, включая встречи и конференции. Для процедурных слушаний предпочтение отдается полностью виртуальным форматам, но респонденты предпочли бы оставить возможность личных слушаний открытыми для слушаний по существу, а не чисто дистанционное участие. Респонденты проявляют готовность перейти на безбумажные методы, такие как производство документов в электронной форме, а не в печатном виде; предоставление представлений, доказательств и корреспонденции в электронном формате и использование электронных слуховых аппаратов. Многие респонденты также приветствовали бы более «зеленое» руководство со стороны трибуналов и в форме мягкого права.

Меры и инструменты IT-безопасности, которые чаще всего используются или рекомендуются респондентами, включают «облачные платформы для обмена электронными или электронными данными»; «ограничение доступа к назначенным лицам», «шифрование данных» и «управление доступом, например, многофакторную аутентификацию».

Пандемия COVID-19 с ее карантинными мерами привлекла особое внимание к обеспечению международными арбитражными центрами возможности быстрого разрешения споров [13]. Так, Арбитражный суд ICC в апреле 2020 г. выпустил Руководство МТП о возможных мерах, направленных на смягчение последствий пандемии COVID-19 [14], которое инкорпорировано в Пояснения для сторон и ар-

битражных судов о проведении арбитража в соответствии с Регламентом ICC (Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration) от 1 января 2021 г. [15]. Документ содержит пояснения по применению Арбитражного регламента ICC, включая вопросы виртуального слушания и представления документов в электронном виде.

К аналогичным выводам пришли участники опроса Стокгольмской торговой палаты (SCC) – 77 % штатных юристов в скандинавских компаниях считают выбор метода разрешения споров стратегическим решением на уровне руководства. Опрос также указывает на то, что международное арбитражное сообщество готово перейти на цифровые технологии. Эксперты по разрешению споров, арбитры и стороны, имеющие опыт арбитражных процессов, высоко ценят беспрепятственную цифровую связь, которую обеспечивает Арбитражный институт SCC. Основной задачей Института является сохранение гибкости и рентабельности арбитража в свете все более сложных дел и сложных международных отношений. Дальнейшая цифровизация будет способствовать быстрому и эффективному вынесению арбитражных решений без ущерба для качества. Цифровые методы работы рассматриваются как способ упростить процесс и минимизировать затраты сторон. Многие респонденты также указывали на необходимость сокращения количества поездок с целью снижения их негативного воздействия на окружающую среду [16].

Таким образом, и арбитражное сообщество, и участники арбитражного разбирательства (стороны, эксперты, свидетели, переводчики и др.) положительно оценивают результаты, достигнутые в цифровизации арбитражного разбирательства, и намерены развивать данный современный способ разрешения споров.

Список литературы

1. Статистика МКАС при ТПП РФ за 2021 г. // ОЭР. URL: https://mkas.tpprf.ru/ru/Stat/page.php (дата обращения: 10.09.2022).

2. В субъектах Российской Федерации расширяется деятельность отделений МКАС // ОЭР. URL: https://mkas.tpprf.ru/ru/news/v-subektakh-rossiyskoy-federatsii-rasshiryaetsya-deyatelnost-otdeleniy-mezhdunarodnogo-kommercheskog-i437375/ (дата обращения: 10.09.2022).

3. Сайт ЮНСИТРАЛ // ОЭР. URL: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ru/lg_e-fundstransfer-r.pdf (дата обращения: 10.09.2022).

4. Сайт ЮНСИТРАЛ // ОЭР. URL: https://uncitral.un.org/ru/texts/ecommerce/modellaw/electronic_commerce (дата обращения: 10.09.2022).

5. Сайт ЮНСИТРАЛ // ОЭР. URL: https://uncitral.un.org/ru/texts/ecommerce/modellaw/electronic_signatures (дата обращения: 10.09.2022).

6. Сайт ЮНСИТРАЛ // ОЭР. URL: https://uncitral.un.org/ru/texts/ecommerce/conventions/electronic_communications (дата обращения: 10.09.2022).

7. Сайт ЮНСИТРАЛ // ОЭР. URL: https://uncitral.un.org/ru/texts/ecommerce/modellaw/electronic_transferable_records (дата обращения: 10.09.2022).

8. 2022. 1-й Инструментарий стандартов для трансграничной безбумажной торговли (2022 Standards Toolkit for Cross-border Paperless Trade) // ОЭР. URL: https://www.wto.org/english/res_e/booksp_e/standtoolkit22_e.pdf Авторы Emmanuelle Ganne (WTO) Hannah Nguyen (ICC DSI) (дата обращения: 10.09.2022).

9. Федеральный закон от 29.12.2015 № 382-ФЗ (ред. от 27.12.2018) «Об арбитраже (третейском разбирательстве) в Российской Федерации». СПС «Консультант Плюс».

10. Закон РФ от 07.07.1993 № 5338–1 (ред. от 30.12.2021) «О международном коммерческом арбитраже» (вместе с «Положением о Международном коммерческом арбитражном суде при Торгово-промышленной палате Российской Федерации», «Положением о Морской арбитражной комиссии при Торгово-промышленной палате Российской Федерации»). СПС «Консультант Плюс».

11. Сайт Международной торговой палаты // ОЭР. URL: https://iccwbo.org/content/uploads/sites/3/2017/03/icc-information-technology-in-international-arbitration-icc-arbitration-adr-commission.pdf (дата обращения: 10.09.2022).

12. Обзор международного арбитража // ОЭР. URL: https://arbitration.qmul.ac.uk/research/2021-international-arbitration-survey/ (дата обращения: 10.09.2022).

13. Гайдаенко-Шер Н. В. Удаленный арбитраж в эпоху неопределенности: панацея или дополнительная возможность? // Международный коммерческий арбитраж. 2020. № 2 (4). С. 40–52.

14. Гайдаенко-Шер Н. И. // Международный коммерческий арбитраж. 2020. № 2 (4). С. 52–28.

15. Сайт Международной торговой палаты // ОЭР. URL: https://iccwbo.org/content/uploads/sites/3/2020/12/icc-note-to-parties-and-arbitral-tribunals-on-the-conduct-of-arbitration-english-2021.pdf (дата посещения: 12.09.2022).

16. Сайт Арбитражного института Стокгольмской торговой палаты // ОЭР. URL: https://sccinstitute.com/about-the-scc/news/2022/scc-survey-shows-positive-approach-to-digitalized-working-methods/?link_id=qHK2r62ljF (дата обращения: 30.08.2022).

Н. В. Винник,
старший преподаватель,
Дальневосточный институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

ЦИФРОВАЯ ЮРИДИЧЕСКАЯ КЛИНИКА КАК СУБЪЕКТ ОКАЗАНИЯ БЕСПЛАТНОЙ ЮРИДИЧЕСКОЙ ПОМОЩИ

Аннотация. Статья посвящена вопросам создания цифровой юридической клиники как субъекта оказания бесплатной юридической помощи. При изучении темы автор использовал такие методы научного познания, как анализ, прогнозирование и логический метод. Автор делает вывод о том, что будущее бесплатной юридической помощи тесно связано с активным применением цифровых техно-

логий и внедрением цифровых решений в практику правового консультирования (например, оформление электронного обращения в органы власти, электронного искового заявления, проект «Цифровой юрист» и др.).

Ключевые слова: бесплатная юридическая помощь, правовое консультирование, цифровые технологии, государственные услуги, правовая защита, цифровая юридическая клиника, юридическое образование

DIGITAL LEGAL CLINIC AS A SUBJECT OF PROVIDING FREE LEGAL ASSISTANCE

Abstract. The article is devoted to the issues of creating a digital legal clinic as a subject of providing free legal assistance. In the course of the research, such methods of scientific cognition as analysis, forecasting and the logical method were used. The author concludes that the future of free legal aid is closely connected with the active use of digital technologies and the introduction of digital solutions into the practice of legal advice (for example, the registration of an electronic appeal to the authorities, an electronic statement of claim, the Digital Lawyer project, and others).

Keywords: Free legal assistance, Legal advice, Digital technologies, Public services, Legal protection, Digital legal clinic, Legal education

Право получать бесплатно юридическую помощь гарантировано Конституцией Российской Федерации (ст. 48) и отнесено к абсолютным правам человека, которые не могут быть ограничены законом [1]. Защита прав и свобод граждан – это предмет совместного ведения Российской Федерации и ее субъектов. Система бесплатной юридической помощи урегулирована Федеральным законом о бесплатной юридической помощи [5], а также соответствующими ему законами субъектов России. Законодательство определяет круг субъектов, уполномоченных оказывать правовую помощь нуждающимся гражданам. К числу субъектов относятся юридические клиники, созданные при вузах, осуществляющих подготовку профессиональных юристов. Будущие юристы получают опыт правового консультирования под руководством опытного преподавателя, а нуждающиеся граждане – бесплатную юридическую помощь.

С конца позапрошлого столетия в юридическом сообществе нашей страны обсуждались предложения о необходимости дополнения классического образования практической деятельностью студентов под руководством преподавателей. Ключевые положения клинического образования были выработаны российскими учеными-правоведами в начале XX в. и основывались на опыте стран англосаксонской правовой семьи [2]. При этом многие региональные высшие учебные заведения, создавшие юридические клиники, применяют формы работы прошлого века.

Бесплатную юридическую помощь можно рассматривать как сервисную функцию государства, обеспечивающую единый стандарт прав человека, а также равноправие граждан перед законом и судом. По своей природе общественные отношения по поводу оказания бесплатной правовой помощи являются публично-правовыми, поскольку преследуют социально значимые общественные, а не

частные цели. Тем самым юридические клиники берут на себя часть государственной функции. По данному направлению государство через Министерство юстиции курирует юридические вузы.

Тенденция на применение цифровых и дистанционных технологий в коммуникации прослеживается уже более десятка лет. Юридическое образование и профессиональная деятельность юриста не могут быть в стороне от этого тренда. Клиники относятся к негосударственной системе оказания юридической помощи. Возможно, в этом и кроется причина отставания юридических клиник в вопросах цифровизации от государства.

Многие государственные услуги можно получить с помощью цифровых технологий, что существенно экономит время и повышает эффективность государственных услуг. По многим направлениям созданы единые стандарты оказания государственных услуг в социальной сфере с применением цифровых технологий [3]. Указом Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» обеспечение прав граждан на доступ к информации (в том числе правового характера) определен как стратегический принцип развития государства. Одна из целей Стратегии состоит в развитии человеческого потенциала и социальной сферы [4. С. 33–36]. Подобные цели на сегодняшний день недостижимы без цифровизации системы бесплатной юридической помощи.

Опыт дистанционного образования в период локдауна повлиял на формы работы юридических клиник. Большинство из них перешли на дистанционное правовое консультирование с применением цифровых технологий. Консультирование осуществлялось через электронную почту, телефонную и видеосвязь. Юридические клиники старались использовать все доступные каналы связи. При этом за период дистанционного обучения полноценной «Цифровой юридической клиники» не возникло. Представляется, что ее появление должно стать следующим этапом клинического образования и оказания правовой помощи.

Пандемический период можно считать переходным. Он выявил некоторые коммуникативные сложности, которые преодолеваются через создание Цифровой юридической клиники:

1) усложнен сбор информации;

2) сложнее наладить контакт с собеседником;

3) сложно установить границы профессионального и личного;

4) сложно соблюдать временные рамки и придерживаться графика;

5) сложнее контролировать работу студентов-консультантов.

В настоящее время идет становление «Виртуальной юридической клиники» как явление в системе бесплатной юридической помощи. Для совершенствования работы юридических клиник, повышения качества правового консультирования и преодоления вышеуказанных трудностей, можно предложить некоторые меры, доступные для большинства российских вузов:

1) вузы могут настроить через собственные официальные сайты опцию подачи электронных обращений, опции обратной связи, а также опции по оценке качества оказанной помощи;

2) при этом на сайте также можно фиксировать статистику поданных и обработанных обращений.

Такой клиенториентированный подход уже применяется органами государственной власти и коммерческими организациями, оказывающими услуги гражданам. Полагаю, что рано или поздно все вузы придут к созданию таких виртуальных кабинетов бесплатной юридической помощи. Обратившийся гражданин сможет самостоятельно, зайдя на официальный сайт юридического вуза, выбрать форму правовой консультации (звонок по телефону, видеосвязь, электронное обращение или запись на личный прием в удобное время). Цифровая юридическая клиника сделает доступнее бесплатную юридическую помощь, позволит экономить время и материально-технические ресурсы вуза, а также повысит эффективность контроля качества такой помощи.

Руководители юридических клиник в период дистанционной работы смогли оценить удобство и эффективность правового консультирования посредством цифровых технологий. Переход к Цифровой юридической клинике можно осуществить только при деятельном участии преподавателей, занимающихся клиническим воспитанием. Руководители и иные работники администрации юридических вузов, занятые своей основной деятельностью, могут упускать из вида вопросы цифрового развития юридических клиник.

Задача руководителя клиники в этой связи состоит в проявлении инициативы и информировании не только администрации учебного заведения, но и федерального органа государственной власти, координирующего оказание бесплатной юридической помощи – Министерство юстиции Российской Федерации. Минюст ежегодно запрашивает у юридических вузов планы мероприятий и отчеты об оказании бесплатной правовой помощи для формирования аналитического материала о состоянии бесплатной юридической помощи в России. Создание Цифровой юридической клиники упростит обмен информацией и автоматизирует подготовку аналитического материала. Работа юридических клиник станет открытой и при этом будет соблюдаться требование защиты персональных данных обратившихся, поскольку информация, размещенная в открытом доступе, будет обезличена.

Так как государство заинтересовано в качественном выполнении государственных функций по оказанию бесплатной юридической помощи юридическими клиниками, Министерству юстиции совместно с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации может быть поручена разработка методических рекомендаций по созданию «Цифровой юридической клиники» с учетом потребностей общества и пожеланий юридических клиник. Реализация такого проекта окажет пользу правовому воспитанию, правовому информированию и правовому просвещению, а также послужит цели укрепления конституционных гарантий равноправия.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства РФ. 2020. № 1. Ст. 4392.

2. О бесплатной юридической помощи в Российской Федерации: Федеральный закон от 21.11.2011 № 324-ФЗ (ред. от 01.07.2021) // Собрание законодательства РФ. 2011. № 48. Ст. 6725.

3. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

4. Писаревский Е. Л. Проблемы применения цифровых технологий при оказании государственных услуг в социальной сфере и пути их решения // Информационное право. 2018. № 3. С. 33–36.

5. Smith R. H. The English Legal Assistance Plan // Significance for American Legal Institutions American Bar Association Journal. June 1949. Vol. 35, № 6. Pp. 453–456, 526–528. URL: https://www.jstor.org/stable/25716880 (дата обращения: 25.07.2022).

Е. П. Волос,
старший преподаватель кафедры гражданского права и процесса,
Московский университет имени С. Ю. Витте

НАСЛЕДОВАНИЕ ИГРОВЫХ АККАУНТОВ

Аннотация. Автором поставлена цель рассмотрения игровых компьютерных аккаунтов в качестве возможных объектов наследственных отношений. На конкретных примерах показано, что в целом ответ на вопрос о наследовании игровых аккаунтов, скорее, отрицательный. В частности, действуют положения из пользовательских соглашений о том, что такой актив не должен передаваться по наследству. Однако возникновение технических средств и отдельного регулирования в ряде стран показывает, что намечается тенденция к установлению возможности передачи игрового аккаунта по наследству.

Ключевые слова: наследование, игровой аккаунт, компьютерный аккаунт, завещание, наследник, цифровое право, цифровые технологии

GAME ACCOUNTS AND THE LAW INHERITANCE

Abstract. The author's purpose is to study if gaming accounts should be considered as possible objects of inheritance. In general, concrete examples show that the answer to the question is rather negative. In particular, according to the provisions of the user agreements game accounts could not be inherited. However, there are countries where technical means and separate regulation are being created. Those cases show that there is a tendency to establish the possibility of transferring a gaming account by inheritance.

Keywords: Inheritance, Gaming account, Computer account, Will, Heir, Digital law, Digital technologies

Мобильные игры и видеоигры на сегодня очень популярны, а приобретение внутриигровых цифровых активов стало обычным действием. В рамках заявленного исследования необходимо выяснить, что происходит с игровыми аккаунтами и прилежащими цифровыми активами после смерти пользователя. Рассмотрим ряд онлайн-игр.

Так, онлайн-игра CryptoKitties, разработанная на базе блокчейна Ethereum, позволяет игрокам покупать, продавать, собирать и разводить виртуальных кошек разных пород. Игра поддерживает стандарт NFT, каждый кот уникален и не может быть воспроизведен. Цена за кошку несколько сотен долларов США, после покупок кошек можно «спаривать» за оплату. Транзакция происходит в сети Ethereum [5]. Игра чем-то похожа на давнюю игру «тамагочи» – нужно следить за биоритмом котиков, чтобы тот «не умер». Соответственно, если говорить о передаче такого актива, в том числе по наследству, то такой котик может «умереть» до его получения в наследство и тем самым наследник может лишиться дорогостоящего актива. Здесь может быть поставлен вопрос о возможности «заморозки» актива или предоставления кому-либо доступа к аккаунту (своего рода душеприказчик).

Из практики разных стран известно, что появляются технические средства, гарантирующие передачу по наследству аккаунтов в компьютерных играх. Например, недавно был выдан патент, на который Tencent Holdings подала заявку в 2019 г. Этот патент, среди прочего, касается наследования цифровых активов. Он позволит напрямую передавать цифровым наследникам учетные записи видеоигр и цифровые активы, если они указаны в завещании [7]. Возможность включения данных цифровых активов в наследственную массу может быть необходима для завещателя, если он совершает внутриигровые покупки в мобильных играх, например, на своих мобильных телефонах или игровых системах, таких как Playstation и Xbox.

Получается, если пользователь умирает, а его учетная запись больше не используется, внутриигровые покупки или другие активы цифровой видеоигры могут оказаться невостребованными. Таким образом, геймер должен заблаговременно подумать, кто из цифровых наследников получит игровых персонажей, статус продвинутого уровня и другие подобные цифровые активы, связанные с игрой.

Китайский законодатель внес поправки в гражданское законодательство, которые влияют и на игровую индустрию. Нормами установлено, что интернет-собственность и виртуальная валюта (и криптовалюта) могут быть унаследованы. Интересно, что сюда также входят игровые аккаунты и виртуальные внутриигровые активы [8].

Другие ученые полагают, что в цифровые активы входят игровые учетные записи, артефакты и персонажи, а также другие ресурсы (например, виртуальные деньги) в играх. Предполагается, что пользователи платят десятки тысяч долларов за вышеуказанные виртуальные ресурсы, а они состоят только из компьютерного кода. Такие ресурсы, составляющие цифровые активы пользователя, должны быть постоянными и невоспроизводимыми, чтобы считаться имуществом [6. С. 7]. Подобная практика уже имеет место, наследие культурного мира существует в ограниченном физическом количестве, однако сейчас возможна продажа объекта в цифровом варианте, например, картина или ваза в единичном физическом экземпляре могут быть оцифрованы в NFT – невзаимозаменяемые токены с предоставлением приватного ключа.

Возникают и различные споры по данной проблеме. Супруга умершего владельца аккаунта игры League of Legends подобрала ответ на секретный вопрос, который задает система игры, если пользователь забыл пароль. Изменив пароль

и секретное слово, она попыталась продать аккаунт и его внутренние цифровые активы. Мать умершего потребовала вернуть наследство, возместить ущерб и признать супругу умершего сына недостойным наследником [9].

Отдельного внимания заслуживают этические аспекты наследования игровых аккаунтов. Довольно-таки прозрачно выглядит наследование, к примеру, если имеет место приобретение цифровых артефактов танка в популярной игре World of Tanks, которое подразумевает в том числе его апгрейд (англ. upgrade – «повышение, улучшение, модернизация»). Однако, к примеру, существуют игры-симуляторы жизни (одна из самых популярных в мире – The Sims), в которых можно создавать персонажей, присваивать им свои имена, возраст, увлечения, создать дом или генеалогическое древо, аналогичное своему настоящему. Получается, историю персонажа можно выдумать, а можно полностью взять факты из своей собственной жизни и продублировать их в игру. В результате цифровой наследник из унаследованного цифрового аккаунта может узнать детали личной жизни наследодателя, например, наличие внебрачных детей, что может после стать фактом доказательства в суде, а не выдумкой пользователя.

Также интересен вопрос с оригинальными дизайнерскими решениями завещателя при выстраивании архитектурных компонентов игры. Правоприменители должны обращаться к законам реального мира только в случае, если события виртуального мира влекут последствия для реального. Данное правило требует конкретизации, поскольку последствия для реального мира можно найти всегда, когда игровое имущество имеет денежный эквивалент и может быть продано на e-Bay или Avito (далее – на рынке), причем независимо от способа приобретения игрового имущества: за деньги или своими силами по правилам игры [3. С. 45]. Так, игровые активы – это «вещи», доступные для покупки пользователями в виртуальной среде (например, игре): костюмы, украшения, домашние животные, аксессуары для строительства и дизайна, техника и оружие и т. д. У большинства перечисленных составляющих есть аналоги в физическом мире.

В пользовательских соглашениях по-разному определяется вопрос о том, могут ли передаваться элементы игры другим лицам, в том числе по наследству. Корпорация Valve является компанией, занимающейся разработкой компьютерных игр. В лицензионном соглашении игры данной корпорации указано, что учетная запись, включая любую информацию, относящуюся к ней (например, контактную информацию, платежную информацию, историю учетной записи, подписки и т. д.), является строго личной. Поэтому возможность продажи и иные способы передачи учетной записи запрещены. Если все же в завещании были указаны игровой аккаунт и активы наследодателя, данные положения завещания являются недействительными, поскольку положения лицензионного соглашения игровой корпорации являются превалирующими [4].

Данную точку зрения подтверждает Г. В. Киселев, отмечая, что владельцы цифровых игровых платформ являются в некотором роде монополистами, которые разрабатывают лицензионное соглашение конечного пользователя. В качестве примера приводится игра MMOG (Massively Multiplayer Online Game), в которой ранее вся торговая деятельность сопровождалась только виртуальной валютой. Сейчас же игро-

вые артефакты, виртуальную валюту возможно обменять на реальную, однако вопрос с обналичиваем средств слабо регламентирован пользовательским соглашением [2].

Виртуальное игровое имущество является частью игры, т. е. программы для ЭВМ. Изображение, которым игровой атрибут символизируется в игре, или код, которым он записан, не представляют ценности вне рамок игры. Данный признак является основной проблемой наделения наследников правами на игровое имущество, поскольку разработчик игры обладает исключительным правом на игру как на объект авторского права [1. С. 62]. Таким образом, при решении вопроса о наследовании аккаунтов в компьютерных играх или элементах компьютерной игры могут быть применены нормы о наследовании интеллектуальных прав.

Как видим, в целом ответ на вопрос о наследовании игровых аккаунтов, скорее, отрицательный. Имеются положения из пользовательских соглашений и доктринальные рассуждения о том, что такой актив не должен передаваться по наследству. Однако возникновение технических средств и отдельного регулирования (к примеру, в Китае) показывает, что намечается тенденция к установлению возможности передачи игрового аккаунта по наследству.

Список литературы

1. Архипов В. В. Интеллектуальная собственность в индустрии компьютерных игр: проблемы теории и практики // Закон. 2015. № 11. С. 61–69.

2. Киселев Г. В. Правовые проблемы наследования игровых аккаунтов в многопользовательских онлайн-играх. Право и бизнес. 2021. URL: http://www.consultant.ru/law/podborki/nasledovanie_akkaunta/ (дата обращения: 03.06.2022).

3. Перепелкина Я. А. Виртуальное игровое имущество: перспективы правового регулирования // Журнал Суда по интеллектуальным правам. 2020. № 3 (29). С. 45–59.

4. Bratt C. What happens to your Steam account when you die? URL: https://www.eurogamer.net/ (дата обращения: 03.06.2022).

5. Jiang H.-J. CryptoKitties Transaction Network Analysis: The Rise and Fall of the First Blockchain Game Mania. 2021. URL: https://www.frontiersin.org/articles/10.3389/fphy.2021.631665/full (дата обращения: 05.05.2022).

6. Meehan M. Virtual Property: Protecting Bits In Context // Richmond Journal o Law & Technology. 2006. № 8. P. 366.

7. Obedkov E. Tencent obtains patent to allow inheritance of digital in-game items // Game World Observer. 2021. URL: https://gameworldobserver.com/2021/07/13/tencent-obtains-patent-to-allow-inheritance-of-digital-in-game-items (дата обращения: 03.06.2022).

8. Tokajian M. L. China’s Civil Code Will Allow Inheritance of Digital In-Game Items. 2021. URL: https://www.top10esports.com/ (дата обращения: 03.06.2022).

9. Williams V. E. Die Frau hat das QQ-Konto ihres verstorbenen Freundes betrogen und die Vermögenswerte des Spielkontos weiterverkauft, die an Familienmitglieder übertragen wurden. URL: https://www-gamingdeputy-com.translate.goog/ (дата обращения: 15.05.2022).

Е. Н. Гладкая,
кандидат юридических наук,
Институт экономики Национальной академии наук Беларуси

К ВОПРОСУ О МЕСТЕ ЦИФРОВЫХ ОБЪЕКТОВ В СИСТЕМЕ ОБЪЕКТОВ ГРАЖДАНСКИХ ПРАВ (НА МАТЕРИАЛАХ ИССЛЕДОВАНИЯ ЗАКОНОДАТЕЛЬСТВА ГОСУДАРСТВ – ЧЛЕНОВ ЕАЭС)

Аннотация. В статье предпринята попытка определения правовой природы цифровых объектов, выступающих объектами гражданских прав. Результаты исследования законодательного опыта государств – членов ЕАЭС, а также трудов отечественных и зарубежных ученых позволили выявить тенденции развития гражданского законодательства на современном этапе. Сформулированные выводы легли в основу авторской концепции, направленной на определение места цифровых объектов в системе объектов гражданских прав.

Ключевые слова: гражданское право, объекты гражданских прав, цифровые объекты гражданских прав, нематериальные объекты, имущество, вещь, бестелесное имущество, цифровые аналоги вещей

TO THE QUESTION OF THE PLACE OF DIGITAL OBJECTS IN THE SYSTEM OF OBJECTS OF CIVIL RIGHTS (BY THE MATERIALS OF THE STUDY OF THE LEGISLATION OF THE EAEU MEMBER STATES)

Abstract. The article attempts to determine the legal nature of digital objects that act as objects of civil rights. The results of the study of the legislative experience of the Eurasian economic integration member states, as well as the works of domestic and foreign scientists, made it possible to identify trends in the development of civil legislation at the present stage. The formulated conclusions formed the basis of the author's concept aimed at determining the place of digital objects in the system of objects of civil rights.

Keywords: Civil law, Objects of civil rights, Digital objects of civil rights, Intangible objects, Property, Thing, Incorporeal property, Digital analogues of things

Введение. Технологический прогресс необратим, и с каждым годом сфера применения его результатов будет только увеличиваться, что подтверждается положениями Национальной стратегии устойчивого развития Республики Беларусь на период до 2035 г., утвержденной протоколом заседания Президиума Совета министров Республики Беларусь от 4 февраля 2020 г. № 3 [21] (далее – Национальная стратегия устойчивого развития Республики Беларусь). В частности, в соответствии с п. 6.1 указанной стратегии, «*В перспективе в стране (в Республике Беларусь. – Прим. автора) будет осуществлена научно-технологическая трансформация экономики с поэтапным переходом к высшим технологическим укладам. Будет создан фундамент общества знаний и интеллектуальной экономики*». Так, в настоящее время в трудах отечественных ученых (Н. С. Минько [18, 19], Н. Г. Колесень [14], М. П. Курилович [18], А. А. Сулейков [18], А. В. Чигилейчик

[26], О. О. Ядревский [27] и др.) углубленному изучению подвергаются отдельные проблемы использования искусственного интеллекта.

Следует отметить, что отсутствие должного правового регулирования указанных процессов может привести к расширению возможностей нарушения прав и законных интересов участников общественных отношений, в том числе общественных отношений, основанных на праве собственности. В связи с этим видится необходимым формирование действенной нормативной правовой базы, способствующей обеспечению прав и законных интересов участников общественных отношений с использованием передовых технологий.

Основная часть. В современных условиях развития информационного общества, становления цифровой экономики и, как следствие, трансформации общественных отношений в целом законодательство Республики Беларусь, как и иных государств – членов ЕАЭС, не успевает своевременно реагировать на подобного рода изменения. В результате чего появляются правовые конструкции, неизвестные ни одной отрасли права, которые в юридической литературе именуются как нетипичные (например, А. Я. Ахмедов «Нетипичные институты гражданского права России: постановка вопроса» [1. С. 127–130]). Так, для участников общественных отношений стало обыденным использование терминов: «аккаунт», «сайт», «домен», «онлайн-игры», «компьютерные персонажи», «электронный кошелек», «электронные деньги», «биткоин», «криптовалюта», «блокчейн» и т. п.

Несмотря на то, что приведенный перечень нетипичных объектов достаточно широк и не является исчерпывающим, интерес для исследования представляют только те, которые, на наш взгляд, имеют признаки объекта вещного правоотношения. Среди таковых следует выделить аккаунты, объекты компьютерных игр и цифровые валюты.

Между тем правовой статус, как и правовой режим отдельных из указанных объектов в законодательстве как Республики Беларусь, так и иных государств – членов ЕАЭС не определен либо его определение носит спорный характер.

Однако широкое распространение подобных продуктов в компьютеризированном обществе требует создания для них подробного и понятного правового регулирования. В противном случае отсутствие такого правового регулирования может быть использовано в неправомерных целях, в том числе для совершения деяний, носящих незаконный характер.

Задачей современной цивилистики нам видится глубокий анализ правовой природы нетрадиционных объектов, являющихся продуктами информационного общества, и возможное определение их места среди иных объектов гражданского права.

Обоснованное признание подобных объектов в качестве объектов гражданского права позволит, в зависимости от их правовой природы, применить к ним необходимый правовой режим, а также решить ряд правоприменительных проблем.

Решение поставленных задач представляется возможным путем реформирования подходов к категории «имущество», с учетом полученных автором результатов исследования в области объекта вещного правоотношения, правомочий собственника и признаков вещных прав [6]. Для получения обоснованных выводов по выбранной теме также особого внимания заслуживает теория о бестелесном имуществе.

В условиях тотального внедрения передовых технологий наибольшему воздействию подвергаются отношения, основанные на праве собственности. Так, с появлением и распространением нетрадиционных объектов интернет-пространства (криптовалюты, аккаунтов, объектов компьютерных игр и т. п.) и невозможностью определения их правовой природы на основании действующего гражданского законодательства Республики Беларусь, представляется актуальным пересмотр имеющихся подходов с учетом положений теории о бестелесном имуществе.

Следует отметить, что деление вещей на телесные и бестелесные берет свое начало со времен римского права. Так, в римском праве под телесными вещами (res corporales) понимали те вещи, до которых можно дотронуться. Таковыми признавались поле, раб, одежда и т. п. Бестелесными (res incorporales) считались те, до которых дотронуться нельзя. К ним, в частности, относились вещи, которые были определены правом, например, наследство, узуфрукт, обязательства [12. С. 324].

Подобные представления о делении вещей сначала нашли свое отражение в философских воззрениях Цицерона, а после в систематике Гая. Цицерон различал вещи, которые существуют (res quae sunt), и вещи, которые мыслятся (res quae intelleguntur). Другими словами, его классификация вещей состояла из материальных предметов и абстрактных понятий. Классификация вещей, по Гаю, состояла из вещей предметного мира и правовых понятий, «…которые представляли предметом требования не сами вещи, но права по поводу вещей» [12. С. 325].

Д. В. Дождев в учебнике «Римское частное право», приводит пример, согласно которому, рассматривая узуфрукт как объект права, римляне могли говорить о его принадлежности лицу наравне с тем, как собственнику принадлежит сама вещь [12. С. 325].

Таким образом, на основании вышеуказанного можно сделать вывод о том, что права в римском праве также могли рассматриваться в качестве бестелесной вещи. Благодаря такому подходу стало возможным формирование категории «нематериальные блага», в которую со временем трансформировалась категория «бестелесные вещи».

Обратим внимание на то, что взгляды современных цивилистов на содержание категории «нематериальные блага» значительно отличаются от тех, которые имели место в римском праве. Возможно, это связано с тем, что гражданское законодательство Республики Беларусь в качестве нематериальных благ признает исключительно те, которые так или иначе связаны с личностью их носителя. В результате чего круг объектов, которые могли бы быть отнесены к нематериальным благам, сильно сужен. Так, в соответствии со ст. 151 Гражданского кодекса Республики Беларусь [9] (далее – ГК Беларуси) к нематериальным благам относятся: жизнь и здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна, право свободного передвижения, выбора места пребывания и жительства, право на имя, право авторства, иные личные неимущественные права и другие нематериальные блага, принадлежащие гражданину от рождения или в силу акта законодательства. При классификации объектов гражданских прав перечисленные объекты причисляют к объектам, не относящимся к имуществу [16. С. 76].

Отдельные ученые отмечают, что перечень личных благ, закрепленный в ст. 151 ГК Беларуси, не является исчерпывающим и может быть дополнен как на основании положений самого кодекса, так и положений иных нормативных правовых актов. В частности, по мнению С. С. Вабищевич, к иным личным благам относится право каждого на достойное отношение к телу после смерти, закрепленное в Законе Республики Беларусь от 12 ноября 2001 г. № 55-З «О погребении и похоронном деле» [23], а также право автора селекционного достижения определять его название (п. 1 ст. 1004 ГК Беларуси) [15. С. 15].

Исходя из изложенного, можно отметить, что современное понимание термина «неимущественное благо», которое заложено в гражданском законодательстве Республики Беларусь и следует из трудов ученых, занимающихся исследованием вопросов гражданского права, утратило то, содержание, которое вкладывалось в понятие «бестелесная вещь» современниками Цицерона, а после Гая.

В настоящее время нематериальные блага рассматривают в двух аспектах: как объекты гражданского права, неотделимые от личности носителя, поскольку являются результатом проявления личных качеств человека (жизнь, здоровье, честь, достоинство и т. п.) и как объекты гражданского права, которые могут быть отделены от субъекта в порядке воплощения их в материальном объекте (произведении науки, литературы и искусства и др.) [15. С. 7; 16. С. 89]. Таким образом, под «нематериальным благом» понимают неовеществленное благо, которое тесно связано с личностью его носителя, как правило, не имеет эквивалентно-стоимостной оценки, а значит, не относится к имуществу с точки зрения законодательно закрепленной классификации объектов гражданского права. По этой причине говорить о возможности применения теории о бестелесных вещах в том смысле, который был заложен в нее еще в римском праве, на данный момент не приходится.

Вместе с этим отдельными учеными предпринимаются попытки возродить отдельные положения теории о бестелесных вещах с целью их последующего применения для регулирования имущественных отношений. По нашему мнению, такой процесс обусловлен ростом значения неовеществленных объектов, использование которых в экономическом обороте постоянно увеличивается. В том числе речь идет об объектах интернет-пространства.

Д. В. Мурзин полагает, что под бестелесной вещью следует понимать субъективное обязательственное право, которое регулируется нормами вещного права. Ученый предлагает к бестелесным вещам, наряду с иными объектами гражданского права, относить ценные бумаги [20. С. 79].

Ю. С. Гамбаров рассматривал бестелесные вещи с позиции интеллектуальной собственности. С его точки зрения, объектами теории о бестелесных вещах в первую очередь должны являться продукты научной, художественной, промышленной и других видов духовной деятельности человека [3. С. 589].

Резюмируя, отметим, что необходимость расширения круга объектов, относимых к бестелесному имуществу, признается рядом ученых. Большинство из них полагает, что, помимо прав, имеющих оценочную стоимость, к бестелесным вещам следует относить оборотоспособные нематериальные блага, переход прав на которые опосредуется извлечением выгоды. Отдельные из них предлагают такие

нематриальные блага признать объектом отношений, выступающих предметом правового регулирования вещного права (например, Д. В. Мурзин).

В то же время некоторыми отечественными учеными оспаривается возможность распространения правовых норм о вещных правах на бестелесное имущество. Так, С. С. Вабищевич, А. А. Гигель указывают, что «…распространение режима вещных прав на объекты, не являющиеся вещами, противоречит самой природе этих объектов» [2. С. 161].

И. А. Маньковский в качестве объектов вещного права рассматривает «…исключительно вещи, под которыми следует понимать созданные природой или трудом человека и материализованные в пространстве объекты, служащие удовлетворению различных потребностей людей» [17. С. 52]. На основании такого определения ученый приходит к выводу, что различные виды энергии, потребляемой через присоединенную сеть, а также результаты интеллектуальной деятельности не могут быть объектами вещных прав по причине отсутствия их материализации в пространстве. Тем не менее ученый допускает, что в случае обретения ими материальной формы они могут рассматриваться в качестве объектов вещных прав (скажем, если энергию заключить в аккумуляторную батарею, то последняя может быть рассмотрена в качестве объекта права собственности).

Между тем если к энергии или результатам интеллектуальной деятельности такого рода материализацию употребить можно, то к иным видам бестелесных вещей, в частности к объектам интернет-пространства, она неприменима. На данный момент нет той материальной формы, в которую можно облечь аккаунт, купленные доспехи для героя компьютерной игры, мегабайты трафика, виртуальный остров и т. п. Устройство, на котором хранятся подобные объекты, не выполняет функцию их материальной формы, поскольку используется не только для этих целей. В противном случае каждый раз при переходе прав на объекты интернет-пространства должны были бы передаваться права на компьютер, мобильный телефон или иное устройство, с которых осуществлялся к ним доступ.

Преобладание среди ученых-цивилистов материалистических представлений о вещи объясняется тем, что длительный период времени указанный объект гражданского права рассматривали исключительно как объект материального мира. Так, О. С. Иоффе в качестве возможных материальных объектов гражданского правоотношения называл «…вещь или иное благо, с которым связано закрепляемое правом общественное отношение и на которое направлено поведение участников правоотношения» [13. С. 221]. В контексте поиска решения проблем собственности И. А. Покровский отмечал, что объектами, находящимися в собственности, могут быть движимые и недвижимые вещи, выступающие правовыми категориями, имеющими материальную форму [25].

Представляется, что в условиях развития информационного общества и цифровой экономики представление о вещи только лишь как объекте материального мира утратило свою актуальность. С расширением возможностей современного человека, в том числе в условиях интернет-пространства, увеличивается количество сфер его деятельности, не имеющих правового регулирования. Игнорирование подобных процессов может привести к правовому коллапсу. В связи с этим особого внимания заслуживают результаты наших предыдущих исследований [4, 5], в со-

ответствии с которыми в странах англосаксонской правовой системы развитие правового регулирования бестелесного имущества строится на основании институтов вещного права, несмотря на то, что большинство таких нематериальных объектов по своей правовой природе относится к субъективным правам. Основанием же для их причисления к бестелесному имуществу (бестелесной вещи) являются их имущественная ценность и отсутствие какой-либо материальной формы. Таким образом, имущественную ценность и отсутствие материальной формы следует рассматривать в качестве своеобразных критериев при отнесении того или иного объекта гражданского права к бестелесному имуществу.

В контексте развития межгосударственных отношений в рамках международной организации региональной экономической интеграции (ЕАЭС) было уделено внимание опыту использования теории о бестелесном имуществе в законодательстве государств-членов (Республики Армения, Киргизской Республики, Республики Казахстан, Российской Федерации).

Результаты исследования показали, что в законодательстве Республики Армения имуществом, наряду с движимым и недвижимым, признаются имущественные права (ст. 132 Гражданского кодекса Республики Армения [8] (далее – ГК Армении)). Право собственности, как и основанные на нем иные гражданские права, именуются имущественными без дополнительной квалификации на вещные (раздел 4 ГК Армении).

В Гражданском кодексе Республики Казахстан [10] (далее – ГК Казахстана) к имуществу отнесены имущественные блага и права, а именно: «…вещи, деньги, в том числе иностранная валюта, финансовые инструменты, работы, услуги, объективированные результаты творческой интеллектуальной деятельности, фирменные наименования, товарные знаки и иные средства индивидуализации изделий, имущественные права, цифровые активы и другое имущество» (п. 2 ст. 115 ГК Казахстана).

В Гражданском кодексе Российской Федерации [11] (далее – ГК России) понятие «имущество» прямо не закреплено, но можно сделать вывод, что оно следует из содержания ст. 128 ГК России. Согласно указанной статье, к объектам гражданских прав относятся: вещи (включая наличные деньги и документарные ценные бумаги), иное имущество, в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права); результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага». Таким образом, в соответствии с ГК России, объекты, обозначенные нами курсивом, следует рассматривать в качестве имущества.

В Гражданском кодексе Киргизской Республики [7] (далее – ГК Киргизии) сохранен традиционный подход к определению перечня объектов, относящихся к имуществу. К последнему, в силу ст. 22 ГК Киргизии, относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права. Аналогичная по содержанию норма содержится в ст. 128 ГК Беларуси.

Применительно к законодательству Республики Беларусь также нельзя не отметить содержание отдельных норм Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» [24] (далее – Декрет № 8),

определяющих правовой статус и правовой режим токенов. В частности, п. 3.4, который свидетельствует о том, что токены для целей бухгалтерского учета являются активами (имуществом); п. 3 Приложения 1 к Декрету № 8, согласно которому токен принадлежит его владельцу на праве собственности или ином вещном праве.

Выводы. На основании проведенного исследования можно сделать следующие выводы:

1. К основным тенденциям развития законодательства Республики Беларусь о вещных правах в условиях широкого распространения передовых (преимущественно цифровых) технологий относятся:

– увеличение роли теории о бестелесном имуществе [5];

– расширение перечня возможных объектов гражданских прав за счет включения в него объектов интернет-пространства и иных цифровых объектов;

– изменение подходов к определению категорий «вещь», «имущество» путем отнесения к ним объектов, не имеющих материальной формы.

2. Имущественные права причислены к имуществу в законодательстве каждого государства – члена ЕАЭС. В законодательстве отдельных государств – членов ЕАЭС (например, в законодательстве Республики Казахстан) перечень объектов гражданских прав, отнесенных к имуществу и не имеющих материальной формы достаточно широк. В связи с этим считаем обоснованным помимо традиционных классификаций имущества (движимое/недвижимое и другие) использование новой классификации – телесное имущество (или имущество, имеющее материальную форму) и бестелесное имущество (т. е. имущество, материальной формы не имеющее).

3. Использование выработанной нами классификации имущества в зависимости от наличия у него материальной формы позволит определить правовой статус и правовой режим объектов интернет-пространства, иных цифровых объектов, выступающих объектами гражданских прав. Так, принимая во внимание специфику имеющегося в Республике Беларусь правового регулирования общественных отношений с использованием цифровых объектов (речь идет о нормах Декрета № 8), предлагается указанные объекты квалифицировать как цифровые аналоги вещей и внести соответствующие изменения в ст. 128 ГК Беларуси [6. С. 31–32].

Список литературы

1. Ахмедов А. Я. Нетипичные институты гражданского права России: постановка вопроса // Вестник Саратовской государственной юридической академии. 2017. № 4 (117). С. 127–130.

2. Вабищевич С. С., Гигель А. А. Личные права организаций со статусом юридического лица // Современные инновационные технологии и проблемы устойчивого развития в условиях цифровой экономики: сб. статей XIII Междунар. науч.-практ. конф., Минск, 24 мая 2019 г. Минск: Колорград, 2019. С. 159–162.

3. Гамбаров Ю. С. Гражданское право. Общая часть / под ред. В. А. Томсинова. Москва: Зерцало, 2003. 816 с.

4. Гладкая Е. Н. Бестелесное имущество: сравнительный анализ подходов к его определению в отдельных странах англосаксонской и романо-германской правовых семей // Современные инновационные технологии и проблемы устойчи-

вого развития в условиях цифровой экономики: сб. статей XIII Междунар. науч.-практ. конф., Минск, 24 мая 2019 г. Минск: Колорград, 2019. – С. 167–175.

5. Гладкая Е. Н. О значении теории о бестелесном имуществе в контексте внедрения передовых технологий (на материалах исследования опыта отдельных зарубежных стран) // Актуальные проблемы гражданского права. 2022. № 1 (19). С. 44–69.

6. Гладкая Е. Н. Основные направления развития вещных правоотношений в контексте внедрения цифровых технологий // Актуальные проблемы гражданского права. 2021. № 2 (18). С. 27–43.

7. Гражданский кодекс Киргизской Республики // Централизованный банк правовой информации Киргизской Республики. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/4 (дата обращения: 17.07.2022).

8. Гражданский кодекс Республики Армения // Законодательство стран СНГ. URL: http://base.spinform.ru/show_doc.fwx?rgn=2998 (дата обращения: 20.06.2022).

9. Гражданский кодекс Республики Беларусь // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. URL: https://etalonline.by/document/?regnum=hk9800218&q_id=5678923 (дата обращения: 20.06.2022).

10. Гражданский кодекс Республики Казахстан // ПАРАГРАФ: информационные системы. URL: http://adilet.zan.kz/rus/docs/K940001000_ (дата обращения: 05.08.2022).

11. Гражданский кодекс Российской Федерации (часть первая) // Некоммерческая интернет-версия КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 26.02.2022).

12. Дождев Д. В. Римское частное право: учебник / под ред. В. С. Нерсесянца. Москва: Издательская группа ИНФРА М–НОРМА, 1996. 704 с.

13. Иоффе О. С. Советское гражданское право. Москва: Юрид. лит., 1967. 494 с.

14. Колесень Н. Г. Теоретические подходы к правовому регулированию искусственного интеллекта в контексте права интеллектуальной собственности // Актуальные проблемы гражданского права. 2021. № 1 (17). С. 108–118.

15. Маньковский И. А., Вабищевич С. С. Гражданское право. Общая часть: в 3 т. Изд. 2-е, стереотип. Минск: Междунар. ун-т «МИТСО», 2016. Т. 3: Личные и вещные права. 392 с.

16. Маньковский И. А., Вабищевич С. С. Гражданское право. Общая часть: учеб. пособие. Минск: Адукацыя і выхаванне, 2014. 232 с.

17. Маньковский И. А., Вабищевич С. С. Личные и вещные права: современное состояние и новые научные подходы: монография. Минск: Междунар. ун-тет «МИТСО», 2012. 336 с.

18. Минько Н. С., Курилович М. П., Сулейков А. А. Место искусственного интеллекта в современной системе знаний и его влияние на политические, экономически, социальные и иные отношения // Право и экономика: сб. науч. тр. / НАН Беларуси, Ин-т экономики. Минск, 2021. Вып. 11. С. 115–132.

19. Минько Н. С. Место искусственного интеллекта в современной системе экономических отношений: некоторые правовые аспекты // Третьи цивилистические чтения памяти профессора М. Г. Прониной: сб. материалов Междунар. науч.-практ. конф., Минск, 18 марта 2021 г. Минск, 2021. С. 169–172.

20. Мурзин Д. В. Ценные бумаги – бестелесные вещи. Правовые проблемы современной теории ценных бумаг. Москва: Статут, 1998. 176 с.

21. Национальная стратегия устойчивого развития Республики Беларусь на период до 2035 г. // Министерство экономики Республики Беларусь. URL: https://economy.gov.by/uploads/files/Natsionalnaja-strategija-ustojchivogo-razvitija-Respubliki-Belarus-na-period-do-2035-goda.pdf (дата обращения: 10.07.2022).

22. Об утверждении программы социально-экономического развития Республики Беларусь на 2021–2025 годы // Министерство экономики Республики Беларусь. URL: https://economy.gov.by/uploads/files/macro-prognoz/Programma-2025-nov-red.pdf (дата обращения: 10.07.2022).

23. О погребении и похоронном деле: Закон Респ. Беларусь от 12.11.2001 № 55-З (ред. от 04.01.2021). URL: https://etalonline.by/document/?regnum=h10100055&q_id=5678965 (дата обращения: 28.07.2022).

24. О развитии цифровой экономики: Декрет Президента Респ. Беларусь от 21.12.2017 № 8 (ред. от 18.03.2021). URL: https://etalonline.by/document/?regnum=pd1700008&q_id=5678991 (дата обращения: 30.07.2022).

25. Покровский И. А. Основные проблемы гражданского права // Некоммерческая интернет-версия КонсультантПлюс. URL: http://civil.consultant.ru/elib/books/23/page_22.html#14 (дата обращения: 21.06.2022).

26. Чигилейчик А. В. Робототехника и системы искусственного интеллекта – субъекты или объекты гражданских прав? // Актуальные проблемы гражданского права. 2020. № 1 (15). С. 114–128.

27. Ядревский О. О. Гражданско-правовые аспекты функционирования искусственного интеллекта // Юстиция Беларуси. 2021. № 8 (233). С. 57–61.

А. В. Захаркина,
кандидат юридических наук, доцент,
Пермский государственный национальный исследовательский университет

ЦИФРОВЫЕ АКЦИИ КАК ЮРИДИЧЕСКАЯ КОНСТРУКЦИЯ

Аннотация. Широкомасштабная цифровизация обусловила появление новых юридических конструкций, которые требуют соответствующего научного осмысления. Целью настоящего научного изыскания выступила постановка вопроса об особенностях такой юридической конструкции, как цифровые акции, являющиеся разновидностью цифровых финансовых активов. В статье в рамках научной дискуссии ставятся такие вопросы, как правовая природа цифровых акций, их место в системе объектов гражданских прав, особенности правового режима и нормативной платформы, допустимость/недопустимость их отождествления с бездокументарными ценными бумагами. Настоящая статья подготовлена в рамках гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук в рамках научного проекта МК-3863.2022.2 «Статуирование цифровых финансовых активов как нового инструмента цифро-

вого гражданского оборота: анализ современного состояния российского законодательства и прогнозирование в условиях посткоронакризиса».

Ключевые слова: цифровизация, цифровые финансовые активы, цифровые акции, юридическая конструкция, правовой режим, нормативная платформа, информационная система

DIGITAL SHARES AS A LEGAL STRUCTURE

Abstract. Large-scale digitalization has led to the emergence of new legal structures that require appropriate scientific understanding. The purpose of this scientific research was to raise the question of the features of such a legal structure as digital shares, which are a kind of digital financial assets. The article raises such issues as the legal nature of digital shares, their place in the system of objects of civil rights, the features of the legal regime and regulatory platform, the permissibility/inadmissibility of their identification with non-documentary securities. This article was prepared within the framework of a grant from the President of the Russian Federation for state support of young Russian scientists – candidates of sciences within the framework of the scientific project MK-3863.2022.2 "Statuization of digital financial assets as a new instrument of digital civil turnover: analysis of the current state of Russian legislation and forecasting in the post-coronocrisis".

Keywords: Digitalization, Digital financial assets, Digital shares, Legal structure, Legal regime, Regulatory platform, Information system

Введение. Цифровизация гражданского оборота, ставшая реальностью в результате позитивации таких цифровых новелл, как электронная форма сделки, цифровые права, в том числе утилитарные цифровые права и цифровые финансовые активы, автоматическое исполнение обязательства путем применения информационных технологий и т. д., требует соответствующей адаптации «классических» институтов гражданского права. Интересно заметить, что цифровые новеллы не хаотичны: последовательность позитивации цифровых новелл обусловлена логикой законодателя. Так, создав правовые условия для исполнения гражданско-правовых обязательств при помощи смарт-контракта, законодатель статуировал цифровые права, а затем их разновидность – цифровые финансовые активы, дифференцированные на четыре вида. Все эти новеллы обусловлены техническими достижениями в IT-сфере, и прежде всего, технологией блокчейн. Как справедливо отмечается в зарубежной научной литературе, вокруг блокчейн-платформ и автоматизированных транзакций возникает новая область права, связанная с интернетом вещей [5. С. 393].

Важно выяснить, каковы особенности применения к цифровым новеллам действующих гражданско-правовых норм, какое место эти новеллы займут в пандектной системе российского гражданского законодательства. В этой связи актуализируется решение первоочередной задачи – моделирования юридической конструкции цифровых финансовых активов как одной из цифровых новелл.

Основная часть. Одним из последствий стремительного развития информационных технологий становится появление новых «цифровых» объектов, рас-

пространение которых в гражданском обороте понуждает законодателя к принятию решения об определении их места в системе объектов гражданских прав. Признание цифровых прав новым самостоятельным видом имущественных прав, получивших «права гражданства» в системе объектов гражданских прав, обеспечивает ученых-цивилистов новыми научными проблемами. Одной из таких проблем является формирование юридической конструкции цифровых финансовых активов. Обозначенная задача не становилась ранее предметом самостоятельных научных исследований и, как следствие, не была подвергнута комплексной разработке.

Изучению вопросов наследования цифровых финансовых активов должен предшествовать хотя бы поверхностный анализ этого нового технико-правового явления. Так, следует заметить, что появление цифровых финансовых активов в структуре цифрового гражданского оборота связано с принятием Федерального закона РФ от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее по тексту – Закон о ЦФА) [2]. Формулируя легальную дефиницию термина «цифровые финансовые активы», законодатель придал им статус «цифровых прав», легальная дефиниция которых в свою очередь заняла самостоятельное место в нормах кодифицированного акта гражданского законодательства – ГК РФ (части первой). Оценивая родовой признак того вида ЦФА, который является предметом настоящего научного изыскания, мы можем предложить следующую терминологическую цепочку: цифровые финансовые активы, удостоверяющие права участия в капитале непубличного акционерного общества, – цифровые финансовые активы – цифровые права – обязательственные и иные права, обусловленные правилами информационной системы. Указанная цепочка в упрощенной форме наглядно демонстрирует истинную родовую сущность исследуемого нами технико-правового явления.

Стоит подметить, что законодатель не дифференцирует цифровые финансовые активы по видам. Вывод о подобной дифференциации мы сделали на основе анализа легальной дефиниции ЦФА и взаимосвязанных норм права (особенно ст. 12–13 Закона о ЦФА). Так, из анализа легальной дефиниции ЦФА следует вывод о возможности их деления на четыре вида по удостоверяемому праву. При этом одним из видов ЦФА выступают цифровые финансовые активы, удостоверяющие права участия в капитале непубличного акционерного общества. Цивилистическая доктрина, стремящаяся к терминологическому упрощению, уже выработала термин, используемый вместо указанного выше громоздкого терминологического ряда, – «цифровые акции» [4. С. 77]. Добившись терминологической определенности, цивилистическая доктрина не преуспела в однозначной правовой квалификации «цифровых акций», правовой режим которых отличается существенной спецификой, обозначенной в ст. 13 Закона о ЦФА. Самую большую сложность вызывает родовая принадлежность цифровых акций. Если исходить из систематического толкования вышеуказанных цифровых новелл, то следует однозначный вывод о том, что цифровые акции – это цифровые права, которые в свою очередь, как уже указывалось, признаны самостоятельным объектом гражданских прав.

Однако в таком случае возникает вопрос о допустимости квалификации цифровых акций в виде ценных бумаг. Очевидно, что решение этого вопроса необходимо и для того, чтобы выяснить особенности их юридической конструкции – идеальной модели, задуманной законодателем. Поскольку законодатель исходит из такого родового признака цифровых акций, как цифровые права, в рамках настоящего научного изыскания мы займем его позицию, признавая, что выявление правовой природы цифровых акций может и должно стать предметом последующих догматических изысканий.

Постулат о том, что цифровые акции – это цифровые права, должен быть признан исходным при выяснении юридической конструкции последних. Нормативная основа юридической конструкции цифровых акций сконцентрирована, главным образом, в правовых предписаниях ст. 13 Закона о ЦФА. Из ее анализа следует вывод о том, что для моделирования юридической конструкции цифровых акций необходимо также апеллировать и к Федеральному закону РФ от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг» (далее по тексту – Закон об РЦБ) [1]. Уже по этому вопросу: какой нормативно-правовой акт первичен по отношению к юридической конструкции цифровых акций – Закон о ЦФА или Закон об РЦБ – в научной литературе возникают дискуссии. Так, в соответствии с п. 3 ст. 13 Закона о ЦФА, эмиссия цифровых акций осуществляется в соответствии с Законом об РЦБ с учетом определенных особенностей. Перечень особенностей, характеризующих юридическую конструкцию цифровых акций с юридико-технической точки зрения, включает в себя восемь пунктов, предлагаемых к поверхностному научному анализу.

Первое. Лицом, ответственным за регистрацию выпусков цифровых акций, выступает оператор информационной системы (далее по тексту – ИС), однако государственная регистрация выпусков цифровых акций не требуется.

Второе. Контентное наполнение решения о выпуске цифровых акций включает в себя следующие сведения: об учете цифровых акций в конкретной ИС; о рисках, сопряженных с приобретением цифровых акций.

Третье. К уставу цифрового акционерного общества, которое, к слову говоря, может быть создано только в форме непубличного акционерного общества, предъявляются специальные требования в части наличия информации об учете цифровых акций в ИС. Учитывая тот факт, что непубличное акционерное общество, выпускающее акции в цифровом виде (в виде цифровых акций), задумано законодателем как «цифровое» акционерное общество (подтверждение тому можно обнаружить в норме п. 1 ст. 13 Закона о ЦФА), очевидно, что и способы созыва, способы проведения общего собрания акционеров, способы уведомления акционеров об осуществлении корпоративных действий могут быть обусловлены ИС. В таком случае соответствующие положения должны быть включены в устав такого акционерного общества.

Четвертое. Тот факт, что акционерное общество выпускает именно цифровые акции, очевидно, должен быть обозначен в уставе соответствующего юридического лица. При этом, как уже отмечалось, законодатель презюмирует, что непубличное акционерное общество должно быть изначально цифровым, т. е. выпускать

с самого начала своей хозяйственной деятельности именно цифровые акции. Это предопределяет необходимость включения соответствующего правила в текст устава непубличного акционерного общества с момента его учреждения. Для усиления аргументации законодатель специально добавляет: «Соответствующие положения не могут быть внесены в устав, изменены и (или) исключены из устава по решению, принятому общим собранием акционеров такого общества». Это нормативное предписание, думается, ограничивает корпоративную свободу, присущую корпоративным отношениям. Такое ограничение обусловлено необходимостью моделирования определенной конструкции цифровых акций, концептуализированной в нормах Закона о ЦФА отечественным законодателем.

Пятое. В продолжение вышеуказанных рассуждений относительно особого «цифрового» статуса непубличного акционерного общества, осуществляющего эмиссию цифровых акций, добавим еще одно положение о таком обществе: оно не может быть преобразовано в публичное акционерное общество.

Шестое. «Цифровое» непубличное акционерное общество не вправе выпускать нецифровые акции. Это правило обуславливает нормативное предписание о недопустимости выпуска иных эмиссионных ценных бумаг, за исключением цифровых акций, в том числе конвертируемых. Конвертируемые ценные бумаги в контексте настоящих рассуждений – это эмиссионные ценные бумаги, выпущенные в любой форме и имеющие способность к конвертации в цифровые акции. Предполагаем, что законодатель ввел прямой запрет на выпуск конвертируемых акций во избежание обхода закона об изначальной «цифровой» природе непубличного акционерного общества, выпускающего цифровые акции.

Седьмое. Не допускается даже в случае реорганизации конвертация цифровых акций в иные акции.

Восьмое. И наоборот: не допускается даже в случае реорганизации конвертация нецифровых акций в цифровые.

Выводы. Резюмируя вышеизложенное, обозначим основные выводы, тезисно отражающие суть научного изыскания, осуществляемого нами.

Законодатель, обеспечив отечественный правопорядок новым корпусом норм, создал новую юридическую конструкцию – цифровые акции, правовой режим которых остается не до конца прозрачным. Так, непонятна правовая природа цифровых акций: понятно, что они квалифицированы в качестве цифровых прав, однако неясно, можно ли их приравнять к известным отечественному правопорядку формам объективации ценных бумаг – например, бездокументарным ценным бумагам. При положительном ответе на данный вопрос цифровые акции могут быть квалифицированы в качестве сложно-структурной конструкции, обладающей одновременно двумя родовыми признаками – цифровые права и бездокументарные ценные бумаги. Усложнение общественных отношений вполне способно осложнять и традиционные объекты гражданских прав, однако затронутая проблема требует дополнительных догматических изысканий.

Если же ответить на поставленный нами вопрос отрицательно, то неизбежно встает вопрос о критериях дифференциации цифровых акций и бездокументарных ценных бумаг, особенно с учетом того, что Совет при Президенте РФ по

кодификации и совершенствованию гражданского законодательства в своем экспертном заключении подметил, что правовой режим цифровых прав и цифровых финансовых активов был сконструирован на основе правового режима бездокументарных ценных бумаг [3].

Список литературы

1. О рынке ценных бумаг: Федеральный закон РФ от 22 апреля 1996 г. № 39-ФЗ (ред. от 14.07.2022) // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата опубликования: 14 июля 2022 г.).

2. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон РФ от 31 июля 2020 г. № 259-ФЗ // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата опубликования: 31 июля 2020 г.).

3. Экспертное заключение по проекту Федерального закона № 419059–7 «О цифровых финансовых активах и о внесении изменений в отдельные законодательные акты Российской Федерации»: принято на заседании Совета при Президенте РФ по кодификации и совершенствованию гражданского законодательства 29 ноября 2018 г. № 182–3/2018 / В данном виде документ опубликован не был // Доступ из СПС «КонсультантПлюс» (дата обращения: 19 сентября 2022 г.).

4. Шевченко О. М. Правовая природа акций, выпускаемых в виде цифровых финансовых активов // Предпринимательское право. 2022. № 1. С. 75–80.

5. Casado-Vara R., Prieto J., De la Prieta F., Corchado J. M. How blockchain improves the supply chain: Case study alimentary supply chain // Procedia Comput. Sci. 2018. Vol. 134. Pp. 393–398.

Е. А. Кириллова,
кандидат юридических наук, доцент,
Юго-Западный государственный университет
Т. Э. Зульфугарзаде,
кандидат юридических наук, доцент,
Российский экономический университет имени Г. В. Плеханова

ОСОБЕННОСТИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ НАСЛЕДОВАНИЯ АККАУНТА, РАЗМЕЩЕННОГО В СОЦИАЛЬНЫХ СЕТЯХ

Аннотация. В данной статье рассмотрены возможность и особенности наследования аккаунта в социальных сетях. В настоящее время все более актуальным становится вопрос о том, что произойдет с учетной записью пользователя после его смерти, вопрос для наследников является актуальным, так как аккаунт может хранить объекты интеллектуальной собственности, а также быть источником дохода. Основная цель исследования заключается в определении правовой природы аккаунта в социальных сетях и возможности передать его содержимое по наследству. В исследовании даны авторские определения цифрового завещания

аккаунта, сделан вывод о том, что аккаунт в социальных сетях является объектом гражданских прав. Содержание аккаунта в некоторых случаях является результатом интеллектуальной деятельности и средством получения дохода, поэтому его можно классифицировать как цифровое наследство, которое может переходить к наследникам по закону и завещанию.

Ключевые слова: аккаунт, социальные сети, завещание, наследники, интеллектуальная собственность, авторское право, цифровизация

FEATURES OF LEGAL SUPPORT FOR INHERITANCE OF AN ACCOUNT POSTED ON SOCIAL NETWORKS

Abstract. This article discusses the possibility and features of inheriting an account in social networks. Currently, the question of what will happen to the user's account after his death is becoming more and more relevant, the question for heirs is relevant, since the account can store intellectual property objects, as well as be a source of income. This situation is due to the novelty of hereditary legal relations in the digital environment. The main purpose of the study is to determine the legal nature of the social media account and the possibility of inheriting its contents. The study gives the author's definitions of the digital testament of an account, and concludes that an account in social networks is an object of civil rights. The content of the account in some cases is the result of intellectual activity and a means of generating income, so it can be classified as a digital inheritance, which can pass to heirs by law and will.

Keywords: Account, Social networks, Will, Heirs, Intellectual property, Copyright, Digitalization

Современное общество интегрировано в цифровую среду, благодаря которой многие осуществляют различную деятельность дистанционно, заключают договоры, ведут электронный документооборот, имеют виртуальный бизнес, обучаются, покупают различные товары. С помощью сети Интернет граждане оформляют учетные записи в социальных сетях и осуществляют деятельность онлайн, включая общение, поиск информации, рекламу. Как показывают статистические данные, более 4,2 миллиарда человек в 2021 г. имели аккаунты на одной или нескольких платформах, это чуть больше половины населения нашей планеты [3]. В таких обстоятельствах учетная запись в социальных сетях с помощью, которой граждане могут осуществлять основные действия в сети Интернет имеет особое значение, а ее правовой статус требует комплексного анализа. Как справедливо отмечают некоторые исследователи учетная запись (далее – аккаунт) является цифровой интеллектуальной собственностью [8. С. 129]. Аккаунт часто используется для получения дохода, поэтому некоторые ученые пошли еще дальше, назвав аккаунты цифровой недвижимостью XXI в. [6. С. 3–4].

Действительно, как показывает практика, аккаунт в социальной сети может приносить владельцу достойный доход от рекламы и прямых продаж. При оформлении статуса самозанятого на странице своего аккаунта в социальных сетях можно рекламировать товары, услуги и таким образом обретать клиентскую базу. В других случаях аккаунты, которые не приносят дохода, могут быть приравнены

к интеллектуальной собственности, так как владельцы размещают на своих страницах собственные творческие материалы в виде прозы, стихов, рисунков и др.

Вопрос распоряжения аккаунтом в социальных сетях на случай смерти редко обсуждается экспертами, на законодательном уровне правоотношения в данной сфере не регламентированы, поэтому необходимо выяснить является ли аккаунт собственностью граждан, зарегистрировавших их на свое имя, может ли аккаунт быть передан по наследству, если да, то каким образом наследники смогут получать доход, если таковой имелся, какие права возникают у наследников на творческие авторские произведения и если владелец аккаунта не оставил завещания с паролями и кодом доступа, как наследники могут вступить в права наследования? Все эти вопросы нуждаются в детальном рассмотрении с целью наметить пути законодательных решений в данной области.

Цель исследования – рассмотрение правового статуса аккаунтов в социальных сетях, способы и возможность их наследования.

Учетная запись в социальной сети (аккаунт) – это аутентификационная запись в компьютерной системе, позволяющая идентифицировать гражданина как пользователя и содержащая сведения как личные, так и не связанные с личностью пользователя. Аккаунт в социальных сетях позволяет хранить и распространять различную информацию, а пользователи сети Интернет воспринимают аккаунт как интернет-ресурс, тесно связанный с личностью владельца аккаунта.

Вопрос правового статуса аккаунта в социальных сетях является дискуссионным, исследователи обсуждают, является ли учетная запись объектом гражданских прав, какова природа пользовательского соглашения, какие права и обязанности могут быть унаследованы [9]. Необходимо отметить, что в данной статье речь идет о персонифицированных аккаунтах, т. е. зарегистрированных на свое имя и вся информация на таком аккаунте, как правило, связана с личностью владельца. Существуют и неперсонифицированные аккаунты, которые продают или даже дают в аренду для пользования, такими аккаунтами пользуются кратковременно, желая скрыть «цифровые следы» в сети Интернет.

Рассматривая аккаунт как объект гражданских прав, некоторые эксперты отмечают, что аккаунты следует относить к нематериальным благам [7]. Отчасти соглашаясь с данным мнением, можно привести следующие аргументы в пользу признания аккаунтов нематериальными объектами: аккаунты, как и нематериальные блага, возникают по факту создания, они тесно связаны с личностью и неотчуждаемы, не обладают экономическими характеристиками. Признавая, что аккаунт в социальных сетях относится к нематериальным благам и может вовлекаться в гражданские правоотношения, следует отметить, что термин «нематериальные блага» не совсем отражает суть аккаунтов. Более точно их можно определить как цифровой объект, который содержит цифровую информацию в виде программного кода, он нематериален и не нуждается в материализации для вовлечения в гражданский оборот, имеет трансграничный и наднациональный формат.

Как указывалось ранее, содержимое аккаунта может быть разным, если дифференцировать аккаунты на виды, то можно выделить следующие:

– аккаунты, которые созданы для общения онлайн;

– аккаунты, маркетинговой направленности с целью получения дохода;
– аккаунты, содержащие творческий материал, объекты авторского права;
– базы данных.

В случае если признать аккаунт в социальных сетях объектом гражданского права, можно распространить на него принципы наследования по аналогии с наследованием неимущественных прав, но в данном случае, можно применять нормы о наследовании по завещанию, если владелец аккаунта распорядился им, предоставив коды доступа в завещании [5. С. 523–532]. Каким образом можно наследовать аккаунт по закону, предстоит определить, проблема заключается в осведомленности наследников о наличии аккаунта и о возможности получить доступ к аккаунту.

Рассмотрим аккаунт в социальных сетях как объект гражданского права, который может составлять цифровое наследство с различных позиций. В случае если учетная запись создавалась для общения онлайн, она может представлять для родственников духовное наследие, содержащее фотографии, видео, личные записи, очень ценные материалы. Разве можно не передать по наследству родным письма и альбомы с фотографиями? Ответ однозначный – это сделать необходимо. Аккаунты в социальных сетях в силу своих особенностей и возрастающего значения способны формировать аудиторию, создавать клиентские базы, некоторые аккаунты имеют миллионную аудиторию, благодаря этим особенностям они часто используются в рекламе. В отдельное направление деятельности выделился социальный медиамаркетинг, когда сотрудники фирм и частных предприятий с целью продвижения товаров и услуг ведут профессиональные блоги в социальных аккаунтах. Размещение рекламы, постоянное освещение направлений деятельности фирмы на личных страницах аккаунтов часто являются должностной обязанностью работника. Таким образом, аккаунт является маркетинговым инструментом для повышения продаж определенных товаров и услуг, данная деятельность взаимовыгодна, так как работники получают процент с продаж, при условии что товары приобретаются благодаря рекламе, размещенной на страницах личных аккаунтов.

Однако владельцы аккаунтов могут и самостоятельно рекламировать свой инфобизнес, приносящий доход, это может быть, например, создание сайтов, копирайтинг, мультимедиапродукция и многое другое, в таком случае унаследовать аккаунт можно, но, чтобы получать доход, наследники должны продолжить предпринимательскую деятельность, для этого необходимо иметь соответствующую специализацию, предпринимательские навыки.

Аккаунт может содержать объекты авторского права, права на результаты интеллектуальной деятельности включают права имущественные и личные неимущественные, которые не могут отчуждаться, – право на имя, авторство, репутация. Необходимо учитывать, что результатом интеллектуальной деятельности будет не сам аккаунт, а авторский контент на который у автора возникают ограниченные авторские права. Авторские права ограничены пользовательским соглашением, в соответствии с которым операторы социальных сетей могут заблокировать аккаунт или ограничить доступ к нему.

Как результат интеллектуальной деятельности, аккаунт в социальных сетях можно отнести к произведениям науки, литературы, искусства или к базе данных.

Если рассматривать страницы аккаунта как произведение, то ее следует классифицировать в качестве так называемых вторичных произведений – сложных объектов или составных произведений.

При наследовании прав на аккаунт как составного произведения следует доказать, что страница – это не просто совокупность отдельных составных элементов – постов (текстов, в том числе иллюстрированных, видеороликов, фотографий, гиперссылок на другие страницы в сети Интернет и т. д.), а что указанные элементы страницы являются материалами, подбор и расположение которых представляют результат творческого труда. При этом сами элементы страницы необязательно должны быть самостоятельными произведениями, а автору составного произведения в соответствии с законом принадлежат авторские права на осуществленные ими подбор или расположение материалов (составительство). С точки зрения расположения и подбора контента страница в аккаунте аналогична интернет-сайту и поэтому может быть также отнесена к составным произведениям.

В случае если отдельные элементы страницы являются самостоятельными объектами авторских прав, страница может рассматриваться как сложный объект. При этом из закрытого перечня сложных объектов аккаунт в социальных сетях следует отнести к мультимедийным продуктам, поскольку страница в социальных сетях отвечает признакам сложности, виртуальности и интерактивности. В случае наследования прав в отличие от составного произведения не нужно будет доказывать творческий характер подбора и расположения элементов. Дополнительно нужно будет обосновать права на сложный объект, которые вытекают из смысла договоров об отчуждении исключительного права или лицензионных договоров на отдельные результаты интеллектуальной деятельности, входящих в сложный объект. На страницах аккаунта могут размещаться и другие результаты интеллектуальной деятельности, однако в ч. 1 ст. 1225 ГК РФ содержится исчерпывающий список охраняемых результатов интеллектуальной деятельности, но аккаунта в данном списке нет. Целесообразно дополнить указанную статью, расширив список таким охраняемым результатом интеллектуальной деятельности, как аккаунт в социальных сетях, содержащий авторский контент творческого характера.

В таком случае наследники получают право на использование творческих произведений и распоряжение ими, т. е. они смогут тиражировать произведения, переносить их на бумажные носители, дарить и даже извлекать доход.

Аккаунт в социальной сети может наследоваться и в качестве базы данных, под базой данных понимается совокупность структурированной и систематизированной информации, хранящейся в памяти компьютера. База данных является объектом смежных прав. Аккаунт в социальных сетях представляющий рекламу товаров в интернет-магазине, может являться базой данных данного магазина, если на страницах аккаунта использованы теги, которые позволяют осуществлять поиск и сортировку информации. Согласно действующему законодательству, изготовителю базы данных принадлежит исключительное право пользоваться материалами базы данных, но при этом необходимо понимать, что ее создание требует

финансовых вложений и серьезных трудовых затрат. Как правило, база данных должна содержать не менее десяти тысяч самостоятельных информационных элементов, которые составляют ее ядро. База данных охраняется законом от несанкционированного использования информационных составляющих. В случае если аккаунт в социальных сетях представляет собой базу данных, он может входить в состав наследства как объект интеллектуальной собственности в цифровом виде. Создатель базы данных должен иметь документы, подтверждающие финансовые вложения в созданный актив, при возникновении спора в суде будет необходимо доказать не только финансовые затраты, но и определить содержимое социального аккаунта как базу данных, а не просто информационный ресурс. Чтобы доказать, что аккаунт является базой данных, владельцу необходимо:

– соответствующим образом оформлять и подписывать договоры со всеми лицами, которые принимают участие в создании страницы;

– оформлять права на информационное наполнение контента;

– вести учет расходов на создание аккаунта в виде базы данных, оформить результат интеллектуальной деятельности как нематериальный актив.

Проведенный анализ позволяет сделать вывод, что содержание аккаунта в некоторых случаях является результатом интеллектуальной деятельности и средством получения дохода, поэтому его можно классифицировать как цифровое наследство, которое может переходить к наследникам по закону и завещанию. При этом, составляя завещание, пользователь имеет такие же права, как при составлении завещания в отношении своего имущества, т. е. он имеет право указать одного или нескольких наследников, распределить наследственные доли дохода поровну или в определенных долях, указать в качестве наследника родственника или лицо, не состоящее с ним в родстве. Во владение указанным имуществом могут вступить сразу несколько наследников. При этом передаче подлежат не все права. Не могут наследоваться права, связанные с личностью автора. Наследники не получают права на изменение результата труда или его публикацию под своим именем. Автор способен передать наследникам по завещанию или по закону исключительные и иные интеллектуальные имущественные права на результаты своего труда. Они наследуются в общем порядке, как и другое имущество и права наследодателя.

Однако возникает вопрос, каким образом следует закрепить за наследниками права на обладание аккаунтом, которые по определению может составлять цифровое наследство. В России аккаунты в социальных сетях не признаются имуществом граждан, а соответственно, нормы права, регламентирующие официальный порядок составления и исполнения завещания, не распространяются на аккаунты. В странах Западной Европы и США вопрос наследования аккаунтов в социальных сетях частично урегулирован. Так, в Испании в Законе о защите персональных данных есть отдельная статья, в которой определен порядок написания завещания, содержащего доступ к аккаунтам [4]. В США в 2005 г. был принят Закон о предоставлении доступа к электронной почте умершего ближайшим родственникам [1], на основе данного законодательного акта позже в разных штатах были приняты специальные правовые акты, которые позволяли получить доступ родственникам

не только к электронной почте, но и к аккаунтам, блогам, электронным кошелькам. Однако в подавляющем большинстве случаев, если владелец аккаунта не распорядиться своим аккаунтом, оставив завещание с паролями и кодами доступа, то предоставление такого доступа социальными сетями по просьбе родственников будет нарушать пользовательское соглашение. Поэтому дела о доступе к аккаунту после смерти владельца решаются в судах. Пользовательские соглашения социальных сетей не регламентируют ситуации передачи аккаунта в наследство родственникам в случае смерти пользователей, в таких соглашениях лишь указано, что страница может быть заблокирована, если пользователь размещает материалы, пропагандирующие насилие, терроризм и другую преступную деятельность.

Судебных прецедентов в данной сфере достаточно мало, в пример можно привести опыт стран Западной Европы, когда Федеральный Верховный суд Германии постановил, что необходимо признать право родственников на наследство в виде аккаунта, дело стало прецедентным, но и повод обратиться в суд у родственников был серьезный, так как девочка-подросток покончила жизнь самоубийством и необходимо было знать с кем непосредственно перед кончиной она общалась, не повлияли ли группы, пропагандирующие суицид, на ее решение. Суд также был заинтересован в установлении контактов подростка перед смертью, поэтому и было принято решение о возможности предоставить доступ к аккаунту родственникам [2. С. 515–522]. Поскольку в рассмотренном случае повод для предоставления доступа к аккаунту и оформление на него наследственных прав был очень серьезным, можно предположить, что в других случаях суд не всегда будет на стороне наследников.

Правовой вакуум подтолкнул социальные сети к разрешению ситуации в случае смерти владельца аккаунта, но эта вынужденная мера и в силу того, что решения очень разные, они со временем должны быть консолидированы, в то же время социальные сети могут предложить лишь порядок функционирования аккаунта, после того как стало известно о смерти владельца, т. е. придать новый статус и функционал страницы, никакие проблемы наследования они урегулировать не в состоянии, и, конечно, это не их прерогатива. Например, «Фейсбук»* официально принял решение предоставлять возможность пользоваться аккаунтом родственникам пользователя, при условии что они предоставят документы, подтверждающие смерть пользователя, и напишут заявление о желании вести блог в аккаунте. При получении всех документов и положительном решении вопроса администрацией «Фейсбука»* аккаунт может перейти под управление родственников с пометкой «мемориал». Разработчики данных правил не разъясняют, каким образом наследники могут получить доступ к странице пользователя, если он им не оставил необходимых для активации страницы паролей, можно предположить, что администрация «Фейсбука»* решит этот вопрос.

Компания Google предлагает пользователям самим решать, что станет с их цифровым наследством, указав период неактивности, после которого компания обязана удалить аккаунт или передать его родственникам пользователя. Период

*Признан экстремистской организацией и запрещен в РФ.

неактивности устанавливается от трех месяцев до полутора лет, но, прежде чем закончится данный период, компания обязана проинформировать пользователя о том, что его аккаунт будет удален или передан родственникам, если пользователь не откликнется, и с его страницей поступят, так как он указал.

Twitter* предложил запустить приложение, которое будет генерировать записи пользователя на основе анализа его интересов, после его смерти, данное приложение пользователь должен подключить при жизни. На основании каких данных и фактов должно запуститься данное приложение, неясно, как показывает статистика, предложение не пользуется спросом – с момента запуска проекта прошло девять лет и пользователи не проявили интерес к данному предложению. Кроме того, следует отметить, что предложение компании Twitter не рассматривает права наследников, которые могли бы получить в наследство аккаунт в социальной сети, и поэтому, возможно, не представляет практической значимости.

«Живой Журнал» детально описывает процедуру присвоения аккаунту статуса «мемориальный»: для его получения наследники должны обратиться в компанию, представить документы, подтверждающие факт смерти владельца аккаунта, после этого аккаунт будет обозначен как «мемориальный», при этом пользователи смогут оставлять комментарии к записям владельца аккаунта.

Таким образом, наиболее крупные компании предпринимают попытки решить проблему аккаунтов в социальных сетях, которые остаются после смерти владельца. Однако если квалифицировать аккаунты как цифровые объекты гражданского права, которые могут входить в состав наследства, то и все вопросы, возникающие в данной сфере, должны быть регламентированы на законодательном уровне. Компании могут со своей стороны решать вопросы придания определенных статусов неактивным страницам, но решить проблемы наследования они не могут.

Возможно, следует предоставить владельцам аккаунтов при регистрации самим решать, что станет с аккаунтом в социальных сетях и кому, на каких условиях он может быть передан. Делать это можно в процессе регистрации пользователя в сети с возможностью дальнейшего изменения выбранного варианта.

Необходимо предусмотреть и возможность наследования по закону. Родные покойного должны иметь право по закону пользоваться всеми материалами страниц в аккаунте, они также имеют право на доход, который может приносить данный аккаунт. После смерти пользователя наследники должны обратиться по адресу социальной сети, в которой размещен аккаунт покойного, с просьбой присвоить аккаунту определенный статус. Можно предложить три вида посмертных статусов:

– мемориальный с правом оставлять комментарии;

– памятный с запретом на комментарии;

– замороженный с закрытием доступа.

В случае, когда аккаунт приносил определенный доход пользователю, наследники имеют право на получение данного дохода. Составленное цифровое завещание, каково бы ни было его содержание, само по себе никакого наследственного правоотношения не порождает. Оно выступает лишь как первичный юридический факт, который в сочетании с другим юридическим фактом – открытием цифрового

наследства – приводит к возникновению наследственного правоотношения: наследники по завещанию призываются к наследованию.

Выводы. Аккаунт в социальных сетях является объектом гражданских прав. Содержимое аккаунта в социальной сети может составлять цифровое наследство – это результаты интеллектуальной деятельности и связанные с ними имущественные и некоторые личные неимущественные права, а также доход, полученный от деятельности, проводимой в аккаунте наследодателем, которые после его смерти переходят к наследникам по завещанию или по закону. Как результат интеллектуальной деятельности, аккаунт в социальных сетях можно отнести к произведениям науки, литературы, искусства или к базе данных.

Если рассматривать страницу аккаунта как произведение, то ее следует классифицировать в качестве «вторичных» произведений – сложных объектов или составных произведений.

Цифровое завещание аккаунта в социальных сетях – это распоряжение гражданина относительно содержимого аккаунта на случай смерти, сделанное путем указания наследников в соответствующих документах, размещенных в социальной сети, в которой зарегистрирован аккаунт наследодателя. Пользователь имеет право завещать содержимое аккаунта, представляющее собой результаты интеллектуальной деятельности, и доходы, которые пользователь получал в процессе пользования аккаунтом, одному или нескольким лицам, независимо от того, относятся ли они к числу его наследников по закону, а также юридическим лицам.

Необходимо регламентировать на законодательном уровне возможность наследникам управлять аккаунтом и присваивать аккаунту один из посмертных статусов:

– мемориальный (с правом комментировать ранее опубликованные записи);

– памятный (с запретом оставлять новые комментарии);

– замороженный (с полным закрытием доступа к аккаунту).

Список литературы

1. An act concerning access to decedents' electronic mail accounts. Public Act No. 05–136. Substitute Senate Bill No. 262. June 24, 2005. URL: https://www.cga.ct.gov/2005/act/Pa/2005PA-00136-R00SB-00262-PA.htm (дата обращения: 19.07.2022).

2. Cayce Myers. An analysis of social media ownership litigation between organizations and PR practitioners // Public Relations Review, 2015. Vol. 41, Iss. 4. Pp. 515–522.

3. Digital 2021: главная статистика по России и всему миру. URL: https://spark.ru/user/115680/blog/74085/digital-2021-glavnaya-statistika-po-rossii-i-vsemu-miru (дата обращения: 19.07.2022).

4. Incluye las correcciones de errores publicadas en BOE núms. 90, de 14 de abril de 2000. Ref. BOE-A-2000–7052 y 180, de 28 de julio de 2001. Ref. BOE-A-2001–14758. URL: https://www.boe.es/buscar/act.php?id=B0E-A-2018–16673 (дата обращения: 19.07.2022).

5. Kirillova E. A., Blinkov O. E., Lyalin D. Y., Rybakov V. V., Ulybin V. A. Legal status and inheritance of modern digital objects // Astra Salvensis. 2018. № 6 (12). С. 523–532.

6. Блинков О. Е. О судебной практике по делам о наследовании // Наследственное право. 2019. № 2. С. 3–4.

7. Данченко Г. М. Правовое регулирование аккаунта в социальных сетях // Вопросы российской юстиции. 2021. № 16. URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-akkaunta-v-sotsialnyh-setyah (дата обращения: 19.07.2022).

8. Санникова Л. В., Харитонова Ю. С. Цифровые активы: правовой анализ: монография. Москва: 4 Принт, 2020. 304 с.

9. Харисова И. Р., Шлыгина Е. А. Наследование аккаунтов социальных сетей // Ученые записки Тамбовского отделения РоСМУ. 2021. № 24. URL: https://cyberleninka.ru/article/n/nasledovanie-akkauntov-sotsialnyh-setey (дата обращения: 19.07.2022).

А. В. Колосов,
кандидат юридических наук,
Иркутский государственный университет

LEX INFORMATICA: ПОНЯТИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Аннотация. В статье анализируется концепция lex informatica как основа регулирования современных международных торговых отношений в области электронной коммерции и бизнеса. Быстрое развитие информационных технологий, создание современных компьютеров, повсеместное распространение сети Интернет обусловили возникновение новых подходов к осмыслению существующего традиционного права. Ответом на подобные вызовы современности стало появление свода правил, направленных на регулирование торговых операций в информационной среде, которые получили название lex informatica. Автором рассматриваются причины появления, круг источников и перспективы развития lex informatica. Делается вывод, что lex informatica регулирует не только материально-правовое взаимодействие участников договорного отношения, но и процессуальные стороны сотрудничества, а также призвано помочь удовлетворить потребности субъектов предпринимательской деятельности с учетом эволюции торговых отношений в информационной сфере.

Ключевые слова: lex informatica, lex mercatoria, информационные отношения, информационная среда, информация, международный коммерческий арбитраж, типовой закон, торговля, предпринимательство

LEX INFORMATICA: CONCEPT AND PROSPECTS OF DEVELOPMENT

Abstract. The article analyzes the concept of lex informatica as the basis for regulating modern international trade relations in the field of e-commerce and business. The rapid development of information technologies, the creation of modern computers,

the ubiquity of the Internet space have led to the emergence of new approaches to understanding the existing traditional law. The answer to such challenges of our time was the emergence of a set of rules aimed at regulating trade operations in the information environment, which were called lex informatica. The author examines the reasons for the appearance, the range of sources and prospects for the development of lex informatica. It is concluded that lex informatica regulates not only the substantive and legal interaction of the parties to the contractual relationship, but also the procedural aspects of cooperation, and designed to help meet the needs of business entities, taking into account the evolution of trade relations in the information sphere.

Keywords: Lex informatica, Lex mercatoria, Information relations, Information environment, Information, International commercial arbitration, Model law, Trade, Entrepreneurship

Быстрое развитие информационных технологий, создание современных компьютеров, повсеместное распространение сети Интернет обусловили возникновение новых подходов к осмыслению существующего традиционного права.

Появление новых видов электронных договоров, использование компьютерных технологий и возникновение цифровой информации привели к осознанию того, что вновь возникающие общественные отношения в киберпространстве не всегда могут быть эффективно урегулированы имеющимися нормами права и требуется создание новых способов их упорядочивания с учетом динамично развивающейся современной практики в сетевой среде.

Сетевое пространство становится одним из основных средств коммуникации и площадкой для создания, реализации и прекращения экономических, торговых, финансовых и иных видов отношений. Подобные отношения зафиксированы в цифровой форме и осложняются тем, что информация, являющаяся их предметом, может пересекать границы государств молниеносно и быть доступной неограниченному кругу лиц с территории разных стран.

Трансграничный характер отношений и проблема определения территориальной принадлежности, сложность установления связи с правом конкретной страны, которое необходимо применить для регулирования, наличие большого количества иностранных элементов приводят к предложению в научной литературе разнообразных способов регламентации информационных правоотношений.

По мнению отдельных ученых, вновь возникающие отношения в информационном пространстве ничем не отличаются от ранее существовавших, так как все технические устройства и сеть Интернет являются лишь инструментами для их фиксации и передачи информации. В связи с этим киберпространство и появляющиеся отношения должны регулироваться традиционными правовыми способами и существующими нормами, несмотря на появляющиеся технические новшества [2. С. 8].

В противоположность классическому подходу, другие авторы отмечают, что современные технологии невозможно урегулировать существующими нормами и требуется совершенной иной вариант осмысления информационных отноше-

ний и интернет-пространства [1. С. 20]. Основная идея сводится к тому, что к киберпространству и возникающим в нем отношениям правовые средства не применимы, так как лежащий в их основе алгоритмический код – это и есть закон, который регламентирует все протекающие социологические и технологические процессы [3. С. 713]. Таким образом, регулирование отношений в информационном пространстве главным образом осуществляется с помощью технических правил, инструкций и регламентов, которые помогают в их реализации с учетом алгоритмического кода конкретной электронной программы, платформы или вида информационного отношения.

Приведенные точки зрения актуальны и обоснованы. Вместе с тем необходимо нахождение компромисса, который позволил бы учесть преимущества всех приведенных позиций.

Компьютерные технологии и возникающие информационные отношения обладают новизной и требуют применения новых подходов для их регулирования. Однако идея о том, что компьютерный код является единственно возможным способом их регламентации, представляется ошибочным. Информационное пространство, компьютерные программы и новые технологии появляются благодаря деятельности человека, и компьютерный код, который лежит в основе функционирования программ, выполняет операции, которые были определены людьми и являются результатом их деятельности. В то же время нельзя полностью согласиться и с представителями классических взглядов на право, которые настаивают на незыблемости и нерушимости правовых норм и возможности регулирования современных информационных отношений уже существующими правовыми актами. Такая позиция крайне ограничена существующими рамками правового регулирования и не берет во внимание научно-технический прогресс и динамично развивающиеся информационные отношения. Появление технологий блокчейн, смарт-контрактов, криптовалюты, международных транзакций и иных взаимодействий посредством сети Интернет требуют создания более гибких подходов правового регулирования и нахождения компромиссных решений.

В связи с новизной информационных отношений и высокой активностью их развития возрастает роль негосударственного регулирования или так называемого саморегулирования. Существующие классические подходы регулирования не всегда способны учитывать особенности взаимосвязей в киберпространстве, так как зачастую отсутствует комплексный подход в вопросах прав и обязанностей субъектов информационных отношений, объектов их взаимодействия, а также имеется сложность правовой защиты участников.

С целью решения данных проблем и создания унифицированных правил взаимодействия субъектов в сетевом пространстве, несмотря на особенности национальных законодательств участников взаимоотношений, возникает частное нормотворчество, и появляются правила, которые регулируют информационные отношения с учетом складывающейся современной практики.

Всемирная история уже знает подобные примеры, когда вновь возникающие отношения, незнакомые на тот период времени обществу, регулировались правилами, которые создавались с учетом складывающейся практики и решали насущ-

ные проблемы участников взаимоотношений. В эпоху Средневековья купцы, которые странствовали по Европе и занимались торговлей, нуждались в правилах, которые бы создавали основу для международной торговли и стирали различия между феодальным, церковным правом и обычаями конкретных регионов с целью установления надежной основы для экономических отношений. Подобной основой стал свод законов, созданный самими заинтересованными субъектами, получивший название lex mercatoria и состоящий из обычаев и практики, не зависящих от местных правил и позволяющих удовлетворить потребности торговцев с учетом особенностей торговых операций.

В эпоху современных технологий участники информационных отношений, которые «путешествуют» по сетевым путям и инфраструктурам, сталкиваются с аналогичными проблемами правовой неопределенности и противоречивости существующих правовых актов разных стран. Подобные проблемы порождают конфликты в правоотношениях, тогда как существующие правила должны обеспечивать стабильность и предсказуемость взаимодействия участников в информационном обществе.

Ответом на подобные вызовы современности стало появление свода правил, направленных на регулирование торговых операций в информационной среде, которые получили название lex informatica. Концепция lex informatica происходит от средневекового lex mercatoria, регулятора международных торговых отношений. Однако в отличие от существовавших правил lex informatica регламентирует отношения в области электронной коммерции и бизнеса. Предполагается, что участники отношений коммерческого характера, использующие сеть Интернет, могут самостоятельно выбирать применимое право и конкретные нормы с целью претворения их в жизнь, как форму саморегуляции без посредничества государства.

Причиной появления lex informatica стала объективная необходимость регулирования активно меняющейся и уникальной глобальной информационной среды, а также отношений, возникающих и развивающихся в интернет-пространстве путем соблюдения складывающихся обычаев и правил, признаваемых во всем мире. Благодаря lex informatica создаются унифицированные правила, способные установить единообразную и предсказуемую практику во взаимодействии субъектов из различных государств, несмотря на их национальное законодательство.

В качестве источников lex informatica выделяется широкий круг правовых норм, среди которых выступают:

Во-первых, основные принципы права. К таковым относят наиболее фундаментальные положения, регулирующие договорный процесс, а также принципы, заимствованные из lex mercatoria, но с учетом специфики информационных отношений. К примеру, принцип pacta sunt servanda – договоры должны соблюдаться, т. е. стороны информационных отношений должны исполнять взятые на себя обязательства и следовать ранее установленным договоренностям. Важное значение имеет принцип недействительности договора, заключенного под влиянием обмана, который устанавливает обязательства для сторон добросовестно исполнять положения договора, не вводя в заблуждение вторую сторону торговых

правоотношений в информационной среде. И иные принципы, которые позволяют установить основу для взаимодействия участников в интернет-среде и облегчить их взаимодействие.

Во-вторых, это международные акты, создаваемые международными организациями, которые позволяют установить единые правила в информационной среде и создать общее правовое регулирование с целью систематизации отношений. Важное значение имеет деятельность Комиссии ООН по праву международной торговли (ЮНСИТРАЛ), которая способствует развитию торговли, в том числе и в электронной среде, создавая унифицированные правила, которые получили название типовых (модельных) законов. Подобные законы разрабатываются с целью создания шаблона правового регулирования конкретной сферы общественных отношений. Например, Типовой закон об электронной торговле преследует цель облегчить ведение торговли с использованием электронных средств, устанавливает эквивалентный правовой режим бумажной и электронной информации, способствует созданию единых правил для устранения препятствий между участниками правоотношений. Типовой закон об электронных подписях вводит необходимые требования о соблюдении процедуры электронного подписания документов, критерии технической надежности электронной подписи и равнозначности с подписью, сделанной от руки.

В-третьих, международные торговые обычаи, которые стали формироваться в информационной области. Большое количество договорных правоотношений постепенно формирует практику, которая становится образцом для субъектов и примером для регулирования конкретных взаимодействий. Например, обычай, связанный с обязательством сторон по шифрованию проводимых торговых сделок и операций, заключаемых в Сети, и отказ от участия в отношениях, если передаваемые информационные данные шифруются недостаточно и есть опасение их разглашения.

В-четвертых, типовые соглашения и контракты, которые появились как образцы для аналогичных отношений в связи с их популярностью в области торговли. Например, Международная торговая палата подготавливает типовые соглашения, которые носят рекомендательный характер и могут быть использованы в качестве шаблона для регулирования определенных отношений. Подобная практика носит положительный характер и позволяет сторонам воспользоваться уже существующими образцами соглашений и адаптировать их для конкретной ситуации.

В-пятых, решения международных коммерческих арбитражей, благодаря которым формируется единая практика разрешения споров в области электронной торговли, отражающая общие подходы к урегулированию конфликтных ситуаций. Определенным недостатком является то, что зачастую решения арбитражей не публикуются и спорящие стороны не заинтересованы разглашать ход разбирательства в связи с наличием коммерческих тайн и иной информации, которая может быть раскрыта при разглашении итогов судебного процесса. Однако создание единой базы решений международных коммерческих арбитражей по спорам в электронной среде способствовало бы формированию единой практики разрешения подобных конфликтных ситуаций и появлению определенности.

Таким образом, lex informatica представляет собой комплекс правил, которые альтернативны традиционным нормам права и могут быть реализованы без помощи государства. Правовые нормы, создаваемые государством, зачастую носят жесткий и порой статичный характер, тогда как практика, создаваемая самими участниками информационных отношений, динамична, обновляема и гибко подстраивается под желания и интересы конкретных субъектов в сфере электронных взаимоотношений и может стать прочной основой для интернет-бизнеса.

Подобный положительный опыт может быть реализован не только в области правового регулирования отношений по сотрудничеству субъектов предпринимательской деятельности, но также и для разрешения споров, которые потенциально могут возникнуть в ходе такого взаимодействия. К примеру, стороны могут использовать lex informatica в контракте как условие для разрешения споров с учетом особенностей их электронного взаимодействия и предусмотреть разрешение конфликта в онлайн-арбитраже. Думается, что такая практика будет весьма популярна и отвечает условиям современных отношений, когда стороны договора не имеют возможности встретиться лично и поэтому взаимодействуют дистанционно.

В связи с этим lex informatica способна регулировать не только материально-правовое взаимодействие участников договорного правоотношения, но и процессуальные стороны их сотрудничества.

Подобные формы объединения нормативного материала приобретают всю большую популярность, и благодаря информационным технологиям стали формироваться lex sportiva (спортивное право), lex constructionis (строительное право), lex laboris (трудовое право) и иные подсистемы, которые в современном мире становятся аналогами средневекового lex mercatoria.

Таким образом, на основании вышеизложенного можно отметить, что благодаря появлению современных технологий и развитию информационного общества происходит процесс перехода от государственного регулирования к частноправовому, когда участники правоотношений самостоятельно, путем применения сложившейся практики, принципов и обычаев осуществляют саморегулирование в сетевой среде. Lex informatica, как правовое явление, призвано помочь такому регулированию и удовлетворить потребности субъектов предпринимательской деятельности с учетом эволюции торговых отношений в информационной сфере.

Список литературы

1. Нужно ли регулировать биткоин? / Э. Сидоренко, А. Савельев, А. Пушков, Р. Янковский и др. // Закон. 2017. № 9.

2. Kablan S. A. Pour une évolution du droit des contrats: le contrat électronique et les agents intelligents. Thèse présentée à la Faculté des études supérieures de l'Université Laval dansl ecadre du programme de doctorat en droit pour l'obtention du grade de docteur en droit (LL.D.) Faculté de droit. Université Laval Québec. P. 8. URL: https://corpus.ulaval.ca/jspui/handle/20.500.11794/19829?locale=en (дата обращения: 11.09.2022).

3. Godefroy L. Le code algorihmique au service du droit // Recueil Dalloz. 12 avril. 2018. № 14/7771. Pp. 713–792.

С. А. Кочкалов,
кандидат юридических наук,
доцент кафедры гражданско-правовых дисциплин
факультета современного права,
Университет мировых цивилизаций имени В. В. Жириновского;
управляющий партнер Юридической фирмы «Бизнес-Советник»;
руководитель Партнерства арбитражных управляющих

ЦИФРОВИЗАЦИЯ И АВТОМАТИЗАЦИЯ РАБОТЫ АРБИТРАЖНОГО УПРАВЛЯЮЩЕГО В ПРОЦЕДУРАХ БАНКРОТСТВА

Аннотация. Динамично меняющиеся реалии современного мира заставляют трансформироваться институт банкротства. Это сказывается на повышенной ответственности арбитражного управляющего в процедурах банкротства. Целью исследования является рассмотрение инструментов цифровизации и автоматизации, применяемых арбитражными управляющими в процедурах банкротства. Автором выявлены недостатки и существенные минусы в процессе цифровизации деятельности арбитражного управляющего, а также предложены пути совершенствования института банкротства в контексте технологического развития.

Ключевые слова: банкротство, арбитражный управляющий, автоматизация работы, цифровизация банкротства, помощник арбитражного управляющего, электронный документооборот, интеграция бизнес-процессов

DIGITALIZATION AND AUTOMATION OF THE WORK OF THE ARBITRATION MANAGER IN BANKRUPTCY PROCEDURES

Abstract. Dynamically changing realities of the modern world force the institution of bankruptcy to transform. This affects the increased responsibility of the arbitration manager in bankruptcy proceedings. The purpose of the study is to consider the tools of digitalization and automation used by arbitration managers in bankruptcy procedures. The author identifies shortcomings and significant disadvantages in the process of digitalization of the activities of the arbitration manager, and also suggests ways to improve the institution of bankruptcy in the context of technological development.

Keywords: Bankruptcy, Arbitration manager, Automation of work, Digitalization of bankruptcy, Assistant to the arbitration manager, Electronic document management, Integration of business processes

Почти за семилетний период действия главы X Федерального закона РФ от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)» (далее – Закон о банкротстве) [1] институт банкротства физических лиц приобрел массовый характер. Согласно статистике Единого федерального реестра сведений о банкротстве (ЕФРСБ), за период существования процедуры потребительского банкротства несостоятельными стали уже 596 426 граждан [2].

Эпидемиологическая обстановка в стране в связи с заболеваемостью COVID-19, осложнение геополитической обстановки, экономический кризис в стране способствуют увеличению неплатежеспособных должников.

Увеличенный спрос на процедуры банкротства физических лиц напрямую сказывается на работе арбитражного управляющего, нагрузка которого возрастает в разы.

Жесткие временные рамки выполнения антикризисных действий, диктуемые императивными нормами законодательства о банкротстве, ужесточение ответственности за малейшее нарушение требований Закона о банкротстве заставляют последнего задуматься о проблеме автоматизации планирования, бизнес-процессов при осуществлении арбитражного управления.

Рассмотрим основные инструменты цифровизации и автоматизации бизнес-процессов по арбитражному управлению в рамках процедуры банкротства.

1. Программа «Помощник арбитражного управляющего» (далее – Программа ПАУ) – продукт, позволяющий арбитражным управляющим автоматизировать работу по сопровождению процедур банкротства.

Несмотря на наличие различных разработок программного обеспечения на российском рынке, Программа ПАУ является доминирующей разработкой отечественного антикризисного софта, полноценно отвечающей потребностям арбитражного управления.

Как Программа ПАУ упрощает работу арбитражного управляющего:

1. Оптимизирует работу:

– Структурирование информации о должнике, имуществе, кредиторах, дебиторах, доходах и расходах, возникших в ходе процедуры. Что позволяет легко находить необходимые данные [3].

– Контроль и планирование рабочих процессов с помощью календарного плана с функцией напоминания о наступлении сроков исполнения.

2. Экономит время на рабочие процессы, подготовку документации:

– В программе содержится более 600 готовых шаблонов документов (отчетов, анализа финансового состояния должника и прочее), которые автоматически заполняются данными благодаря алгоритмам.

– Программа ПАУ обеспечивает документооборот посредством регистрации исходящей и входящей корреспонденции, создания почтовых реестров, реестров договоров и приказов, печати конвертов.

– Сервис позволяет исполнять обязанности реестродержателя (формировать реестр кредиторов, распределять денежные средства).

– Программа организовывает мероприятия (собрание кредиторов, торги).

3. Позволяет всегда быть в курсе тенденций законодательства:

– Программа содержит постоянно обновляемую нормативно-правовую базу российского законодательства и судебную практику в сфере банкротства.

– Сервис также содержит актуальные справочники госорганов.

4. Автоматизирует сдачу отчетов в саморегулируемую организацию.

На сегодняшний день Программа ПАУ – это не только сервис для подготовки правовых документов, но и динамичная платформа антикризисного менеджмента. Значительную роль в этом играют интеграции, внедренные разработчиками со сторонними сервисами.

1. Интеграция с Единым федеральным реестром сведений о банкротстве.

Программа ПАУ имеет доступ к учетной записи арбитражного управляющего на ЕФРСБ, позволяя добавлять на официальном портале шаблоны сообщений и отчетов, предусмотренных Законом о банкротстве.

Доведение процесса раскрытия информации о ходе процедуры банкротства до полной автоматизации – задача выполнимая, однако полностью полагаться на существующую модель взаимодействия с федеральным ресурсом рискованно. Погрешности в работе информационной системы, а также описки (опечатки), допускаемые в официальных источниках, используемых для сбора информации по делу (судебных актах), могут привести к санкциям за несоответствие публикуемых сведений требованиям, установленным законом и уполномоченным органом, и в худшем случае – к лишению статуса арбитражного управляющего.

2. Интеграция с электронной картотекой арбитражных дел «Мой арбитр».

Данная опция предусматривает возможность доступа в карточку судебного дела для получения информации (ознакомление с материалами дела) или для подачи документов в систему арбитражных судов РФ.

3. Интеграция с сервисом BankroTECH.

Сервис BankroTECH предназначен для учета и управления судебными делами и включает в себя основную информацию по делу, даты судебных заседаний, требования кредиторов к должнику и пр.

За счет автоматической выгрузки данных ресурса BankroTECH моментально создается карточка дела Программы ПАУ, заполняются черновики реестровых требований, добавляются известные даты судебных заседаний в календарь программы.

Требуется доработать функционал по своевременному уведомлению рабочей программой о принимаемых судом решениях, что позволит сэкономить время на анализ банкротных дел, сократить вероятность пропуска установленных сроков на опубликование обязательных сведений.

4. Интеграция с сервисом «Почты России».

Данный функционал помогает формировать почтовые реестры для отправки писем посредством государственной почтовой организации.

Учитывая, что до сих пор преобладает консервативный метод отправки корреспонденции при значительных объемах деловой переписки по каждому судебному делу, то давно назрела потребность в создании специальных каналов обмена информацией для участников банкротного процесса в электронной форме. Автоматизация электронных писем, заверенных квалифицированной электронной подписью, сократит временные и материальные затраты на сбор сведений об имущественном положении должника, уведомлении кредиторов о ключевых моментах процедуры и пр.

5. Витрина данных Программы ПАУ.

Интеграция призвана выгружать сведения о процедуре в специальное «облако», выводя информацию за пределы рабочего места, что полезно как для дистанционного доступа владельца программы к базе данных, так и для арбитражного управляющего, имеющего в подчинении несколько помощников, каждый из которых работает в отдельной программе.

6. Интеграция с системой Пробили.Ру (для компаний).

Интеграция с данной системой позволяет получить аналитические бизнес-справки о должнике, кредиторах, дебиторах и других контрагентах на основе баз данных из 14 достоверных источников.

7. Синхронизация с Google-календарем, что позволяет при заполнении параметров процедуры, получить план процедуры со сроками, инструкциями и напоминаниями.

8. Программа ПАУ позволяет импортировать данные из программы «1С: Бухгалтерия» при составлении финансового анализа и учета доходов/расходов арбитражного управляющего по ведению процедуры.

9. Интеграция с клубом арбитражных управляющих, в рамках которого можно воспользоваться чатом арбитражных управляющих и задавать вопросы коллегам, участвовать в обсуждениях.

Развитие Программы ПАУ идет к тому, что арбитражные управляющие самостоятельно могут выбирать тот или иной функционал, ориентируясь на особенности ведения своего бизнеса и выстроенные рабочие процессы.

Однако нельзя не упомянуть и о проблематике использования Программы «Помощник арбитражного управляющего».

Если финансовая ситуация гражданина-должника носит неоднозначный характер, с наличием особых обстоятельств, то полагаться на программное обеспечение финансового анализа без надлежащей последующей интерпретации результатов не стоит, поскольку выводы могут быть некорректными и сводиться к констатации фактов, без оценки финансовых коэффициентов с учетом особенностей финансовых показателей должника.

Также бывает, что в общий доступ выгружается лишь часть сведений о процедуре или некоторые данные обезличены (в целях сохранения конфиденциальности). Арбитражный управляющий не сможет получить целостную картину о судебном деле (стадиях антикризисного управления, количестве обособленных споров, информации об имуществе и пр.).

Чрезмерная монетизация софта также требует дополнительных финансовых затрат со стороны арбитражного управляющего.

Поэтому давно назрела потребность в создании специализированного софта для комплексного планирования ведения арбитражного управления.

2. Система по оптимизации бизнес-процессов. Отчасти поставленные задачи выполняют имеющиеся на отечественном рынке многочисленные системы по оптимизации бизнес-процессов, в частности, система amoCRM [4], адаптированная конкретно под бизнес-процессы арбитражного управления.

На личном примере, в системе amoCRM гибко настраиваются права доступа для сотрудников для редактирования поставленных задач, предусмотрены большие возможности для планирования процедуры.

Но при всем этом amoCRM – это сервис управления продажами, поскольку информационный продукт рассчитан на бизнес с разветвленной системой отделов продаж, активно продающий товары и услуги. Остальным же пользователям система будет недостаточно или излишне функциональной.

Поэтому приспособить указанный сервис (и ему аналогичные) ко всем особенностям арбитражного управления невозможно.

3. Дистанционный формат взаимодействия субъектов банкротства. В рамках выполнения возложенных на арбитражного управляющего обязанностей по формированию конкурсной массы должника взаимодействие с государственными органами осуществляется в дистанционном формате посредством подачи соответствующего электронного запроса. Запрашиваемые сведения поступают дистанционно, подтверждаются усиленной квалифицированной электронной подписью.

Массовый переход на электронный документооборот, при котором широко развита электронная подача документов в суд через сервис «Мой арбитр», возможность участия в судебном заседании онлайн с использованием видео-конференц-связи в порядке ст. 153, 154 Арбитражного процессуального кодекса РФ значительно упрощают работу арбитражного управляющего и экономят его временные ресурсы.

Отсутствие автоматизированных процессов как проблематика взаимодействия арбитражного управляющего с банковским сектором. Несмотря на то, что институт банкротства граждан действует уже почти семь лет, процессы, связанные с получением и распределением денежных средств через банковские структуры, технически не отлажены, лишены какой-либо автоматизации и отнимают у арбитражного управляющего много времени.

Во-первых, незрелость процесса по снятию прожиточного минимума со счетов гражданина-банкрота.

Поскольку у финансового управляющего отсутствует возможность дистанционного управления счетами банкротов (через мобильное приложение), то для снятия со счета гражданина-должника заработной платы/пенсии в качестве прожиточного минимума для дальнейшей выдачи должнику финансовый управляющий должен лично являться в отделения банков.

Финансовый управляющий обращается в банк с заявлением о разблокировке счета для снятия денежных средств. После проведения проверки банк снимает блокировку счета должника, финансовый управляющий снимает наличные денежные средства и подает заявление на блокировку счета во избежание несанкционированных списаний.

Это весьма времязатратный процесс, поскольку разблокировка счета занимает от трех до пяти рабочих дней. То есть финансовый управляющий должен посетить банки два раза: чтобы подать заявление на разблокировку счета и снять денежные средства после разблокировки счета.

Данный процесс, с соблюдением всех бюрократических этапов, происходит ежемесячно на протяжении всей процедуры банкротства (до одного года) и отнимает очень много времени у арбитражного управляющего.

Во-вторых, открытие специального счета гражданина-банкрота в соответствии с требованиями Закона о банкротстве лишено автоматизации, требует личного присутствия финансового управляющего.

В-третьих, бывают ситуации, когда закрытие счета должника можно осуществить только в том отделении банка, где его открывал сам должник, и только при личном визите финансового управляющего.

В-четвертых, существуют банки, которые не выдают денежные средства, а предоставляют финансовому управляющему возможность перевода на любой счет должника, открытый в другом банке, мотивируя отказ предоставлением доступа к счету исключительно клиенту по его биометрическим данным. А поскольку должник в процедуре банкротства доступ к своим счетам иметь не может, то после поступления денежных средств в другой банк процедура разблокировки счета повторяется заново.

В-пятых, в частности, Сбербанк изменил подход к разблокировке счетов должников в процедуре реструктуризации, указывая, что должник сам должен обратиться в банк с заявлением и предоставить оригинал согласия финансового управляющего (либо его личное присутствие), что часто бывает затруднительно.

Вышеуказанное требует приведения банками к единообразию своих внутренних процедур, дополнение функционала мобильных приложений банков, автоматизации рабочих процессов.

Таким образом, главной проблемой автоматизации бизнес-процесса «арбитражное управление» остается недостаточное программное оснащение его центральных действующих лиц – арбитражных управляющих. Имеющиеся инструменты по упорядочению и упрощению ведения дел о несостоятельности (банкротстве) нуждаются в дальнейшем совершенствовании, поскольку функционал профессионального софта должен носить динамичный характер, быть интегрированным в режим реального времени.

В конечном счете это позволит арбитражному управляющему оперативно реагировать на непрерывно возникающие перед ним задачи, не допуская нарушения положений законодательства о банкротстве.

Список литературы

1. Банкротства в России: итоги первого полугодия 2022 и 2 квартала 2022. Статистический релиз Федресурса. URL: https://download.fedresurs.ru/news/Банкротство статрелиз 2 кв 2022.pdf (дата обращения: 14.09.2022).

2. Глава X Федерального закона от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)». СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_39331/02f510a9d6278ed9ba2b1aa9bee8263d1278abf5/ (дата обращения: 14.09.2022).

3. О программе помощник арбитражного управляющего. Русские информационные технологии. URL: https://russianit.ru/products/pau/ (дата обращения: 14.09.2022).

4. О сервисе amoCRM. Сервис по автоматизации бизнес-процессов. URL: https://www.amocrm.ru/ (дата обращения: 14.09.2022).

А. С. Кусков,
магистр юриспруденции, кандидат культурологии,
Саратовская региональная общественная организация
«Центр правовой защиты потребителей»
Н. В. Сирик,
кандидат юридических наук, доцент,
Смоленский филиал Саратовской
государственной юридической академии,
Смоленский филиал Международного юридического института

ЦИФРОВИЗАЦИЯ ДОГОВОРНЫХ ОТНОШЕНИЙ В ТУРИСТСКОМ БИЗНЕСЕ

Аннотация. В работе проанализированы основные тенденции цифровизации договорных отношений в сфере туризма, выделены признаки, особенности и недостатки договоров о реализации туристского продукта, заключаемых в форме электронного документа. Главное внимание уделено проблемам заключения и расторжения электронных договоров в туристском бизнесе и выработке путей их разрешения с целью достижения единообразия нормативно-правового регулирования и судебной практики.

Ключевые слова: click-wrap-соглашение, договор в форме электронного документа, договор присоединения, потребитель, турист, туристский продукт, туроператор, цифровизация, электронная путевка, электронный договор

DIGITALIZATION OF CONTRACTUAL RELATIONS IN THE TOURISM BUSINESS

Abstract. The work analyzed the main trends in the digitalization of contractual relations in the tourism business, highlighted the signs, features and shortcomings of agreements on the sale of a tourist product concluded in the form of an electronic document. The main attention is paid to the problems of concluding and terminating electronic contracts in the tourism, as well as developing ways to resolve them in order to achieve uniformity of legislative regulation and judicial practice.

Keywords: Click-wrap-contract, Contract in the electronic form, Accession contract, Consumer, Tourist, Tourist product, Tour operator, Digitalization, Electronic ticket, Electronic contract

Одной из актуальных тенденций развития российского туристского бизнеса является цифровизация, имеющая множество проявлений – от виртуализации туристских путешествий до цифровизации договорных отношений между туристскими организациями и туристами. Своеобразным стимулом происходящих процессов стали пандемия коронавируса и санкции стран Запада, которые еще более способствуют переводу туристских правоотношений в цифровое пространство, в том числе через заключение договоров в электронной форме.

Проблематика, связанная с заключением договоров в форме электронного документа, активно развивается в цивилистической доктрине. Однако ра-

боты В. К. Андреева, Л. Ю. Василевской, Л. Г. Ефимовой, Х. В. Идрисова, Г. В. Костиковой, М. Ю. Козловой, В. И. Образцовой, А. И. Савельева, О. В. Тимошенко, В. К. Шайдуллиной, Л. В. Щербачевой посвящены применению электронных договоров только в сфере коммерческого оборота (электронной коммерции). Зарубежными правоведами электронные договоры исследуются в качестве одного из основных видов контрактов, заключаемых с участием потребителей (M. Budnitz, K. Chen, J. Dickie, L. Gillies, R. Hillman, N. Lucchi, J. Macleod, H. Micklitz, R. Schulze, S. Tang, J. Tillson, C. Twigg-Flesner, F. Weber, C. Willett).

Актуальна заявленная тематика еще и тем, что практически отсутствуют исследования, связанные с анализом различных аспектов цифровизации договорных правоотношений в сфере защиты прав потребителей, и в частности, в туристском бизнесе. В этой связи своей работой авторы призывают к дискуссии о потенциале, возможностях и проблемах использования договоров, заключаемых в электронной форме при оформлении правоотношений с туристами.

Дискуссионность вышеуказанных вопросов подтверждается материалами судебной практики, где, с одной стороны, уже сделан устойчивый вывод о правомерности и действительности электронных договоров с туристами, в том числе и договоров, заключенных путем «проставления галочки» (именно click-wrap-договорам и будет уделено основное внимание в нашей работе), а с другой – указывается на необходимость учета межотраслевых связей и конкретных обстоятельств дела при рассмотрении споров, связанных с признанием таких договоров недействительными или незаключенными. Не хватает правоприменительной практике и соответствующих разъяснений высших судов.

Действующим законодательством по общему правилу допускается заключение договоров в электронной форме при соблюдении следующих условий: 1) договор составляется в виде одного документа; 2) подписание документа различными способами (их перечень остается открытым), в том числе путем электронной цифровой подписи, обмена письмами, телеграммами, электронными документами или иными данными в соответствии с абз. 2 п. 1 ст. 160 Гражданского кодекса РФ (далее – ГК РФ) (п. 1, 2 ст. 434 ГК РФ) [1].

На возможность заключения договора о реализации туристского продукта в форме электронного документа указано в ст. 10 Федерального закона «Об основах туристской деятельности в Российской Федерации» [2] и п. 14 Правил оказания услуг по реализации туристского продукта [3]. Ростуризмом внесен на обсуждение Проект Федерального закона «О туризме и туристической деятельности в Российской Федерации» [4], согласно п. 1 ст. 43 которого (по состоянию на 13.09.2022) реализация туристического продукта осуществляется на основании договора комплексного туристического обслуживания, заключаемого в письменной форме, в том числе в форме электронного документа.

Анализ названных норм в их совокупности и взаимосвязи, а также учет реальной практики ведения туристского бизнеса позволяют нам выделить следующие распространенные варианты заключения договора о реализации туристского продукта в форме электронного документа:

1) click-wrap-договоры, представляющие собой типовой формуляр, подписываемый путем присоединения к нему через «проставление галочки»;

2) обмен подписанными сторонами скан-копиями договора по электронной почте и через интернет-мессенджеры (Viber, WhatsApp, Telegram и др.);

3) загрузка подписанной скан-копии договора о реализации туристского продукта в личный кабинет туриста на официальном сайте туроператора или в систему бронирования с обеспечением доступа к ней турагентов и туристов;

4) подписание туристом или иным заказчиком договора о реализации туристского продукта квалифицированной электронной цифровой подписью.

При квалификации туристских договоров как договоров присоединения широкое распространение получили click-wrap-договоры, максимально формализующие и упрощающие правоотношения. Такие соглашения стали использоваться в договорных отношениях в США в конце 90-х гг. XX в., и, соответственно, именно в американской доктрине договорного права предложена наиболее удачная их дефиниция: «…соглашение, полностью заключенное в онлайн-среде (в том числе в Интернете) путем нажатия на кнопку “Я согласен” (I accept), в котором определены права и обязанности сторон» [5. P. 14; 6. P. 3–15].

Данная дефиниция позволяет выделить четыре признака соглашений, заключаемых в форме click-wrap: а) полностью исключается стадия преддоговорных переговоров в офлайн-формате; б) договор заключается только в виртуальной или программной среде; в) текст договора содержит все условия и разделы (в том числе устанавливающие права и обязанности сторон), достаточные для признания его заключенным и последующего исполнения; г) заключение договора осуществляется путем совершения действий, связанных с его прочтением, принятием и подписанием через «проставление галочки».

Российская правовая доктрина настороженно восприняла введение click-wrap-соглашений в деловой оборот. Сегодня можно говорить о существовании как минимум пяти подходов к пониманию их правовой природы:

1) договор, заключаемый путем обмена электронными документами, что полностью соответствует нормам ст. 434 ГК РФ и ст. 10 Федерального закона «Об основах туристской деятельности в Российской Федерации»;

2) договор, заключаемый посредством совершения конклюдентных действий, направленных на ознакомление с текстом договора, последующее принятие его условий путем подписания в форме галочки или клика мыши;

3) договор, заключаемый путем присоединения потребителя к типовому его формуляру, размещенному на сайте исполнителя (продавца), что соответствует нормам ст. 428 ГК РФ о договорах присоединения;

4) договор, заключение которого предполагает обязательное последовательное совершение трех действий: ознакомления с текстом (формуляром) договора, обмена электронными документами, необходимыми для его заключения, последующего заключения договора в электронной форме;

5) договоры, заключаемые способом click-wrap, противоречат законодательству, так как, например, возможность их заключения прямо не предусмотрена нормами Закона РФ «О защите прав потребителей».

Учитывая возросшую популярность подобных договоров в сфере защиты прав потребителей, Роспотребнадзор в информации «Об особенностях click-wrap-со-

глашений» [7] указал на правомерность использования и действительность таких договоров, но с оговоркой, что проставление галочки само по себе не свидетельствует о том, что данная подпись была получена в порядке свободного волеизъявления и о наличии у потребителя возможности отказаться от данного условия. Ведомство отметило, что необходимым при заключении такого договора является соблюдение следующих условий:

– потребитель получил полную и достоверную информацию о товаре (услуге), в том числе не переходя дополнительно по ссылкам и документам, сформировал безошибочное представление о полезности товара (услуги);

– потребитель имеет возможность на одной странице ознакомиться с текстом договора, представленного целиком, а также с описанием ценовых или иных условий сделки (существенных условий договора);

– в веб-форме или программном обеспечении отсутствуют заранее проставленные отметки-«галочки», которые сами по себе порождают возникновение юридически значимых последствий, но в то же время потребитель может не обратить на них внимания или не оценить эти последствия.

Однако, говоря о возможных нарушениях, Роспотребнадзор высказался только о правовых последствиях включения в эти договоры условий, ущемляющих права потребителей, или условий, обусловливающих приобретение одних услуг обязательным приобретением других. Нарушения порядка заключения таких договоров Роспотребнадзором никак не квалифицированы.

Отметим, что заключение договоров о реализации туристского продукта способом click-wrap не лишено ряда недостатков.

Во-первых, заключаемые в этой форме договоры не позволяют установить с должной степенью достоверности принятие его условий конкретным лицом, которое в нем указано. В практике турбизнеса для этого используются следующие приемы: прикрепление к договору скан-копии паспорта; подписание договора не только путем проставления галочки, но и через СМС; загрузка скан-копии распечатанного и подписанного договора в личный кабинет туриста или через систему бронирования на официальном сайте туроператора. Однако во всех перечисленных случаях фактически размывается правовой смысл click-wrap-соглашений, так как подписание путем «проставления галочки» отходит на второй план или рассматривается лишь в качестве одного из нескольких способов подписания такого договора, применяемых одновременно.

Во-вторых, как следствие такой формализации заключения туристских договоров, click-wrap-соглашение не позволяет установить и добровольность волеизъявления того лица, которое подписывает договор. Чаще всего этот недостаток актуализируется при подписании сложных (например, многостраничных) договоров, в том числе содержащих обязательные приложения. В подобных случаях от потребителя обычно требуется многократно проставить галочки под всеми существенными условиями, договором в целом, а также всеми приложениями, являющимися его неотъемлемыми элементами.

В-третьих, большинство договоров о реализации туристского продукта являются типовыми договорами, заключаемыми в форме договора присоединения.

Потребитель не может влиять на содержание предложенного ему туроператором (турагентом) договора и лишь выражает согласие со всеми его условиями, в том числе и с условиями о приобретении дополнительных услуг, в которых турист априори не нуждается, но зачастую не может от них отказаться.

Включение таких дополнительных условий в электронный договор ущемляет права потребителей, так как пп. 5 п. 2, п. 3 ст. 16 Закона РФ «О защите прав потребителей» [8] содержит прямой запрет на обусловливание приобретения одних услуг обязательным приобретением других. Включение в договор условий, ущемляющих права туристов, образует состав административного правонарушения (ст. 14.8 КоАП РФ), на что указывает и Роспотребнадзор [9].

В-четвертых, важное значение для определения судьбы электронного договора имеют технические и программные особенности его заключения, на что, к примеру, указывается в правовой доктрине США. Однако названное обстоятельство не нашло своего отражения в разъяснениях Роспотребнадзора. Как показывает практика, наличие у потребителя или исполнителя технических и программных проблем зачастую приводит к различным дефектам стадии заключения договора о реализации туристского продукта способом click-wrap.

Например, в силу технических и программных проблем потенциальный турист в определенной степени лишается возможности ознакомления с полным текстом договора, вынужден вводить требуемые сведения и подписывать договор и его приложения на различных страницах сайта, не может, особенно с экранов планшета и мобильного телефона, обозреть всю страницу сайта с текстом договора, из-за всплывающих окон и подсказок не может убрать или поставить галочки под теми пунктами, которые содержат существенные условия договора, информацию о правах и обязанностях сторон, и т. д.

Это привело к участившимся случаям подачи в суд исков о признании договоров, заключенных в электронной форме, недействительными или незаключенными, что, в свою очередь, требует применения не только правовых норм, регулирующих порядок заключения и исполнения договоров, но и норм информационного и «технического» законодательства (например, отдельных положений федеральных законов «Об информации, информационных технологиях и о защите информации», «Об электронной подписи» и др.).

На приведенные недостатки в некоторых случаях отмечается позитивное и оперативное реагирование законодателя. Так, в Правилах оказания услуг по реализации туристского продукта 2007 г. договор с туристами признавался заключенным с момента его подписания сторонами. В п. 14 новых Правил [3] законодатель, видимо заранее предвидя вышеназванные проблемы, закрепил правило, согласно которому «договор о реализации туристского продукта, составленный в форме электронного документа, считается заключенным с момента оплаты потребителем туристского продукта, подтверждающей его согласие с условиями, содержащимися в предложенном исполнителем договоре».

Такое правило имеет принципиальное значение, так как вводит своеобразный «период охлаждения» – отрезок времени между моментом заключения договора путем клика мыши и моментом внесения потребителем оплаты по указанно-

му договору. Иначе говоря, потребитель имеет полное право передумать – т. е. до момента внесения оплаты по договору заявить односторонний отказ от его заключения без наступления соответствующих правовых последствий. Однако остается неясной судьба договора в случае внесения потребителем оплаты не в полном размере, а в виде аванса. Полагаем, что право отказаться от такого договора должно реализовываться по общему правилу на основании норм ст. 782 ГК РФ и ст. 32 Закона РФ «О защите прав потребителей».

В процессе судебного разрешения споров о действительности click-wrap-соглашений конклюдентные действия потребителя по заключению договора в электронной форме через клик мыши не квалифицируются судом в качестве таковых по умолчанию, так как бремя доказывания проставления галочки или нажатия кнопки «согласен» как выражения потребителем необходимости в заказываемой им услуге возлагается законом на ответчика. Суд должен оценить и иные обстоятельства заключения click-wrap-соглашения – например, достаточность преддоговорной информации, наличие необходимых технических условий, отсутствие в договоре условий, ущемляющих права потребителя, и т. д. Аналогичные требования предъявляются также к договорным приложениям и дополнительным соглашениям, которые оформляются в электронной форме.

Так, переписка между сторонами путем обмена электронными письмами по WhatsApp с направлением туристской организации копий документов и иной информации, необходимых для бронирования тура, а также последующее осуществление оплаты тура явно свидетельствуют о согласовании всех существенных условий договора и получении туристом всей необходимой информации о туристском продукте и туроператоре, его сформировавшем (Апелляционное определение Санкт-Петербургского городского суда от 02.06.2022 № 33–12592/2022). Переписка через интернет-мессенджер Viber признается надлежащим доказательством заключения дополнительного соглашения об изменении условий договора с туристом (Определение Шестого кассационного суда общей юрисдикции от 01.11.2021 по делу № 88–22917/2021).

Исследуя вопрос цифровизации договорных отношений в туризме, нельзя не остановиться на электронной путевке, создание которой в России в качестве механизма контроля за движением средств, переданных туристом туроператору, началось еще в 2014 г. По мнению разработчиков, данный механизм призван обеспечить прозрачность рынка и выступить в качестве гаранта защиты прав туристов, так как внесение данных в систему являлось обязательным условием туроператорской деятельности. Однако нормативное регулирование для функционирования такой системы разработано не было, а после ее создания и последующего тестирования выявлены различные пробелы.

Новая «электронная путевка» – это документ, сформированный в единой информационной системе электронных путевок, на основе сведений, содержащихся в договоре о реализации туристского продукта [10]. Однако не следует путать электронную путевку, представляющую собой цифровую запись в информационной системе, зашифрованную в виде QR-кода, с туристской путевкой, которая является неотъемлемым элементом договора и выдается туристам на руки или предоставляется в форме электронного документа.

Туроператорам с 1 марта 2023 г. вменяется в обязанность предоставление в ЕИС «Электронная путевка» информации обо всех заключенных договорах о реализации туристского продукта. С этой же даты наступает ответственность за неисполнение этой обязанности в сфере международного туризма и с 1 сентября 2023 г. – в сфере внутреннего туризма. В настоящее время государственная информационная система прошла сертификацию и заработала в тестовом режиме, к ней уже подключились многие туроператоры.

Цифровизация данных на платформе ГИС «Электронная путевка» позволит обезопасить туриста от приобретения нелегального туристского продукта и сформирует необходимые для развития туристского бизнеса базы данных, актуальную статистику и инструменты контроля. Кроме того, наличие такой «электронной путевки», на наш взгляд, заметно упростит процесс рассмотрения и разрешения судами споров с туристами о признании договоров, заключенных в форме электронного документа, недействительными или незаключенными.

Таким образом, в сложных политико-экономических условиях возрастает значимость совершенствования существующих и выработки новых инструментов гражданско-правового регулирования цифровизации договорных правоотношений с участием туристов, надлежащего информирования потребителей при заключении ими договора о реализации туристского продукта в электронной форме. Это в дальнейшем позволит избежать значительного количества споров между туристскими организациями и туристами и будет способствовать оптимизации и эффективизации договорного регулирования в сфере туризма.

Действительность click-wrap-соглашений необходимо устанавливать через призму следующих критериев: а) туристу предоставлена возможность предварительного ознакомления с текстом и условиями договора до его заключения; б) турист вправе отказаться от договора до его оплаты, заявлять односторонний отказ от договора не требуется; в) технические условия (доступ к информационным ресурсам, программным продуктам, каналам связи), должны быть достаточными для заключения договора, последующей идентификации субъектного состава договорных отношений и добровольности волеизъявления лица на заключение договора; г) договор и приложения к нему представлены единым массивом текста на одной интернет-странице; д) турист до заключения договора должен иметь возможность отказаться от всех дополнительных услуг, в которых он не нуждается; е) программная или информационная платформы должны позволять распечатать и/или сохранить текст договора и приложений.

Список литературы

1. Гражданский кодекс РФ (часть первая) от 30.11.1994 № 51-ФЗ (в ред. от 25.02.2022 № 20-ФЗ) // Собрание законодательства РФ. 1994. № 32. Ст. 3301.

2. Федеральный закон от 24.11.1996 № 132-ФЗ (в ред. от 28.05.2022 № 148-ФЗ) «Об основах туристской деятельности в Российской Федерации» // Собрание законодательства РФ. 1996. № 49. Ст. 5491.

3. Постановление Правительства РФ от 18.11.2020 № 1852 «Об утверждении Правил оказания услуг по реализации туристского продукта» (в ред. от 06.09.2021 № 1508) // Собрание законодательства РФ. 2020. № 47. Ст. 7551.

4. Проект Федерального закона «О туризме и туристической деятельности в Российской Федерации» (по состоянию на 13.09.2022 не внесен в Госдуму) // СПС «КонсультантПлюс».

5. Stein L. D. Click to accept // Web Techniques. 2001. № 6. P. 14.

6. Buono F. M., Friedman J. A. Maximizing the Enforceability of Click-Wrap Agreements // Journal of Technology Law and Policy. 1999. Vol. 4, Iss. 3. Рз. 3–15.

7. Информация Роспотребнадзора от 05.11.2020 «Об особенностях click-wrap-соглашений» (документ опубликован не был) // СПС «КонсультантПлюс».

8. Закон РФ от 07.02.1992 № 2300–1 (в ред. от 14.07.2022 № 266-ФЗ) «О защите прав потребителей» // Ведомости СНД РФ и ВС РФ. 1992. № 15. Ст. 766.

9. Письмо Роспотребнадзора от 31.08.2007 № 0100/8935–07–32 «Об особенностях правоприменительной практики, связанной с обеспечением защиты прав потребителей в сфере туристического обслуживания» (документ опубликован не был) // СПС «КонсультантПлюс».

10. Федеральный закон от 28.05.2022 № 148-ФЗ «О внесении изменений в Федеральный закон «Об основах туристской деятельности в Российской Федерации» // Собрание законодательства РФ. 2022. № 22. Ст. 3541.

О. С. Лабабуева,
аспирант,
Санкт-Петербургский государственный экономический университет

ОБОРОТ ЦИФРОВЫХ ПРАВ

Аннотация. В статье рассмотрен вопрос об обороте цифровых прав. При анализе практики и гражданского законодательства было выявлено, что на сегодняшний день не все формы договоров и заключаемых сделок подходят для оборота цифровых прав. В статье выявлены пробелы при заключении сделок с цифровыми правами, а также предложено внести изменения в законодательство для устранения пробелов.

Ключевые слова: право, цифровые права, гражданское законодательство, договор, сделки, купля-продажи, мена, наследство

DIGITAL RIGHTS TURNOVER

Abstract. The article considers the issue of the turnover of digital rights. When analyzing the practice and civil legislation, it was revealed that not all forms of contracts and concluded transactions are suitable for the turnover of digital rights today. The article identifies gaps in the conclusion of transactions with digital rights, and it is also proposed to amend the legislation to eliminate gaps.

Keywords: Law, Digital rights, Civil legislation, Contract, Transactions, Purchase and sale, Exchange

В п. 4 ст. 454 Гражданского кодека Российской Федерации (далее – ГК РФ) внесены изменения, допускающие совершение сделок в отношении цифровых

прав. Дополнение п. 4 ст. 454 ГК РФ после слов «имущественных прав» словами «в том числе цифровых прав» фактически легализует сделки с цифровыми правами. Следовательно, оборот цифровых прав повышается, их можно отнести к объектам гражданских прав и применять нормы ГК РФ.

Внесенные изменения, касающиеся цифровых прав, повлекли изменения и в ряд статей гл. 9 ГК РФ, регулирующих отношения по сделкам. В ст. 160 ГК РФ внесены дополнения в части формы сделки, теперь письменная форма сделки считается соблюденной в случае совершения лицом сделки с помощью электронных либо иных технических средств, которые позволяют воспроизвести на материальном носителе в неизменном виде содержание сделки и при точной возможности определить субъектов проводимой сделки.

Согласно правилам системы ПАО «Сбербанк», с цифровыми правами можно совершать следующие сделки: приобретение, погашение ранее выпущенных цифровых прав, а также иные сделки, которые не противоречат российскому законодательству. Появляется вопрос: а какие сделки, не противоречащие законодательству, можно совершать с цифровыми правами, кроме договора купли-продажи? Для ответа на него обратимся ко второй части ГК РФ.

В гл. 31 ГК РФ законодатель урегулировал обязательство по договору мены. Согласно ст. 567 ГК РФ по договору мены передается в собственность один товар в обмен на другой. К такому договору применяются все положения о договоре купли-продажи. Следовательно, если к договору мены применяются правила купли-продажи, то можно применить мену к сделкам по цифровым правам. Однако нормы о договоре мены не применяются к договору купли-продажи. Так, для начала надо будет доказать право собственности на цифровое право. Согласно Постановлению Арбитражного суда Московского округа от 3 июня 2020 г. по делу № А40–164942/2019 право собственности возникает на цифровое право в момент внесения записей в реестр цифровых транзакций в системах [1]. Суд ссылался при таком решении на ст. 2 проекта Закона о ЦФА. Из судебной практики следует, что на цифровое право возникает право собственности.

Также данный факт подтверждает п. 14 ст. 8 Закона о краудфандинге, в котором указано, что можно обменять цифровое право на цифровое право.

Однако в ст. 8 ФЗ о краудфандинге существуют ограничения, в системе можно обменять утилитарное цифровое право на иное утилитарное цифровое право и аналогично цифровым финансовым активом. В случае с меной цифрового финансового актива сумма денежных требований по одному цифровому активу должна быть равна или приблизительно равна другому цифровому активу. Такое условие можно увидеть и в ст. 568 ГК РФ, в которой установлено, что товары при заключении договора мены должны быть равноценными. В законе предусмотрено, что в случае если сумма денежных требований неравноценна, сторона, передающая товар ниже цены товара другой стороны, должна покрыть убытки от такой разницы. Такое правило будет действовать и при мене цифровых прав. Равноценными, по нашему мнению, можно признать такие цифровые права:

– если в случае с утилитарными цифровыми правами, то при мене вид утилитарного цифрового права схож или приблизительно схож. Так, например, если

меняется право требования выполнения работ, то можно совершить обмен только на право требования выполнения работ;

– если в случае с цифровым финансовым активом, то равноценной сделкой по договору мены будет равная сумма по обмениваемым цифровым финансовым активам или приблизительно равная сумма.

Мена может производиться согласно ст. 11 Закона о ЦФА через оператора обмена цифровых активов.

Таким образом, хотя на практике такой договор пока не применяется, договор мены с цифровыми правами может быть заключен.

Следующий возможный вид сделки указан в главе 32 ГК РФ. Глава посвящена договору дарения. Согласно ст. 572 ГК РФ, по договору дарения одна сторона передает безвозмездно другой стороне договора вещь в собственность, т. е. право собственности переходит от одного лица к другому без выполнения денежных обязательств и уплаты разницы в цене. Рассматривая договор дарения относительно цифровых прав, можно сделать вывод о том, что не все цифровые права можно передать по договору дарения. Так, согласно п. 2 ст. 8 Закона о краудфандинге цифровым правом не может быть право, которое требует государственной регистрации или удостоверения у нотариуса. Остальные указанные в п. 1 ст. 8 Закона о краудфандинге виды утилитарного цифрового права можно передать по договору дарения, так как не требуется государственная регистрация.

В ст. 7 Закона о краудфандинге указано, что передача возможна, но только в самой системе с помощью внесения изменений в записи в системе (платформе). Далее, согласно этой статье, как только право передается другому лицу от первоначального лица, у первоначального лица прекращается право собственности. Прекращается оно потому, что оператор системы и он, как предыдущий уже собственник, вносит изменения в записи в системе о передаче цифрового права иному лицу на основании договора дарения. Так, такие положения можно применить и к дарению, и, следовательно, по договору дарения можно передавать цифровые права.

Если цифровые права можно передать по договору мены и дарения, то стоит рассмотреть право наследования цифровых прав.

Согласно ст. 1110 ГК РФ по наследству происходит передача имущества умершего к другим лицам согласно порядку наследования. Согласно ст. 1111 ГК РФ наследование проходит по завещанию или наследственному договору, или по очереди наследования, т. е. по закону, если нет ни договора, ни завещания.

По наследству передается все имущество, которое в указанные документы или находилось во владении умершего в период его жизни. Если у умершего были цифровые права, то их можно передать по наследству. Это связано с тем, что, как было доказано ранее, на цифровые права возникает право собственности, а также ст. 128 ГК РФ цифровые права включены в объекты гражданского законодательства.

Однако возникают некоторые вопросы, которые не учитываются при регулировании передачи по наследству цифровых прав.

Как сказано в первой главе, цифровое право удостоверяет право на другой объект, следовательно, в наследственный договор будет включено само право или

же обозначаемый цифровым правом объект. Закрепление цифровых прав в ст. 128 ГК РФ уже подразумевает, что цифровое право может выступать самостоятельным объектом наследственного завещания или договора.

Также возникают проблемы наследования цифровых прав, которые прикреплены к личному кабинету.

В таком случае вместе с цифровым правом переходит по наследству к наследнику и личный кабинет, в котором хранится доступ к цифровому праву. Для получения доступа к личному кабинету потребуется привести ряд доказательств того, что кабинет принадлежал ушедшему из жизни человеку.

На основании указанного выше порождается проблема: с точки зрения права по завещанию или наследственному договору цифровое право включается в наследственную массу и в дальнейшем передается наследнику, а с технической точки зрения не может быть передано наследнику в том случае, если доступа к личному кабинету нет и не доказано, что кабинет принадлежит умершему, следовательно, это означает, что цифрового права нет у наследника. Однако в п. 2 ст. 4 ФЗ о ЦФА указано, что оператор обязан передавать информацию и вносить изменения не только по требованию обладателя, но по требованию иных лиц. Так, можно будет с точки зрения второй стороны договора или же на основании копии договора на цифровое право потребовать у оператора внести изменения в систему и сменить обладателя цифрового права на наследника цифрового права.

Возможным представляется законодателю рассмотреть особенности технического осуществления цифровых прав, а также проанализировать практику по наследственному праву и внести изменения в законодательство. Так, например, абз. 1 ст. 1112 ГК РФ дополнить словами «и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам».

Возможным представляется дополнить гл. 65 ГК РФ статьей под названием «Наследование цифровых прав», в статье можно будет рассмотреть более подробно выявленные выше проблемы наследования цифровых прав. Включение новой статьи в перечень уже имеющихся статей в ГК РФ позволит урегулировать вопросы наследования благ, созданных в цифровой системе.

В правилах системы, на примере ПАО «Сбербанк», сделки осуществляются с помощью смарт-контракта, в котором указываются все условия сделок с цифровыми правами. Рассмотренные выше сделки из ГК РФ могут осуществляться и в виде смарт-контракта, за исключением передачи наследства. Однако в теории представляется возможным использование смарт-контракта при наследовании.

На сегодняшний день изменений внесено не было. Существует множество мнений по поводу смарт-контракта. А. И. Савельев отмечает, что «смарт-контракт – договор, который составляется в виде кода, существующего на базе блокчейн. Такой договор автоисполняется при наступлении определенных условий» [2. С. 7–14, 32–60]. Если коротко, то, по нашему мнению, смарт-контракт – автоматизированная система исполнения обязательств, т. е. он не выступает привычным нам договором, а является ничем иным, как выражением договора в виде цифрового кода в цифровых технологиях. Для ввода норм о смарт-контракте требуется раз-

решить вопросы о том, кто будет составлять контракт, так как кто-то должен нести ответственность за неправильное составление такого договора. Следовательно, требуется для начала найти решения для указанных вопросов, а потом вводить смарт-контракт в систему договорных отношений РФ.

В указанных выше сделках участвуют субъекты.

Для начала выделим объекты цифровых прав. К объектам относят легализованные на территории Российской Федерации утилитарные цифровые права и цифровой актив. Так, в сделках указывается непосредственно само цифровое право на объекты, которые учитываются и удостоверяются в специальных реестрах с помощью внесения записей в цифровые регистры. Из всего вышесказанного можно сделать вывод, что цифровые права оборотоспособны.

Субъектами сделок могут выступать правообладатели и третьи лица. В качестве правообладателей принято выделять как физических, так и юридических лиц. Таких лиц, согласно указанию Банка России от 25.11.2020 № 5635-У (далее – Указ Банка России), называют квалифицированными инвесторами [4]. Для определения квалифицированного инвестора требуется обратиться к Закону о рынке ценных бумаг. Квалифицированным инвестором, согласно ст. 51.2 Закона о рынке ценных бумаг, является лицо, которое соответствует требованиям, указанным в п. 2, п. 4 ст. 51.2 Закона о рынке ценных бумаг. Следовательно, лица, которые не подпадают под требования закона, являются неквалифицированными инвесторами.

Согласно п. 1 Указа Банка России, только квалифицированные инвесторы могут совершать сделки с цифровыми правами. Физические лица, не являющиеся квалифицированными инвесторами, согласно п. 2 Указа, могут совершать сделки с цифровыми правами через оператора обмена в пределах суммы, передаваемой в качестве оплаты или же в качестве встречного предоставления, не больше 600 тыс. рублей [4]. Данное ограничение распространяется только на совокупность денежных средств, в том числе и на стоимость цифровых прав. Однако юридические лица, не являющиеся квалифицированными инвесторами, могут приобретать цифровые права без ограничений по сумме.

К числу субъектов цифровых прав можно отнести оператора информационной системы, оператора обмена цифровых финансовых активов и оператора инвестиционной платформы. Согласно ст. 10 ФЗ о ЦФА и ст. 10 Закона о краудфандинге, чтобы стать оператором, требуется внести о себе информацию в специальный реестр Банка России, кроме того, предусмотрены квалификационные требования к руководителю и должностным лицам. Так же, как оператор информационной системы, оператор информационной системы может утвердить иные правила. Одно и то же лицо может быть одновременно и оператором информационной системы, и оператором информационных, если оно соответствует требованиям, предъявляемым к этим субъектам (п. 2 ст. 10 ФЗ о краудфандинге).

Оператором информационной платформы может быть, согласно ст. 5 Закона о ЦФА, юридическое лицо, оператором обмена цифровых финансовых активов, согласно п. 2 ст. 10 ФЗ о ЦФА, – кредитные организации, организаторы торговли, а также юридические лица, а согласно п. 4 ст. 10 Закона о краудфандинге – оператором инвестиционной платформы. В указанных статьях содержится открытый перечень требований к операторам.

Все посредники (операторы), с помощью которых осуществляются сделки с цифровым правами, являются юридическими лицами (коммерческие организации), за исключением оператора обмена цифровыми активами. Оператором обмена цифровых активов может быть некоммерческая организация.

Основания привлечения к ответственности в полной мере установлены только для оператора инвестиционных платформ, рассматривая с точки зрения участников и органов юридических лиц операторов инвестиционных платформ. Таким образом, до сегодняшнего дня не проработаны вопросы привлечения к ответственности посредников, участвующих в гражданско-правовых сделках, в случае нарушения прав граждан и юридических лиц.

Возникает проблема при заключении гражданско-правовых договоров на платформе определения субъекта ответственности в случае причинения вреда или ущерба при различных технических сбоях, кражах. Дополнительно возможным видится применять нормы ГК РФ о штрафах и возмещении убытков, а с другой стороны, в зависимости от нарушений, к примеру при краже, можно применять нормы уголовного законодательства или административного, в зависимости от суммы кражи.

Не раскрыт вопрос противодействия отмыванию преступно нажитых денежных средств третьими лицами. В мировой практике цифровые права используются для легализации денежных средств. Имеющиеся положения ФАТФ в Российской Федерации не содержат положений о цифровых правах. Требуется пересмотреть положения и внести изменения на основе практики. Так, например, в п. 15 Рекомендаций ФАТФ требуется добавить после слов «включая новые механизмы передачи» следующую формулировку: «…в том числе иные права, содержание и условия, осуществление которых определяются в соответствии с правилами информационной системы». На основании этой формулировки в дальнейшем можно разработать отдельный новый рискориентированный подход по оценке цифровых прав как способа оценивания возможного использования цифровых прав как средства отмывания преступно нажитых денежных средств и как следствие закрепления в рекомендациях ФАТФ. А также можно будет разработать способы как юридические, так и технические по предупреждению отмывания денежных средств.

Налоговая служба РФ не дает полного ответа на вопрос про исчисление налогов при совершении операции с цифровыми правами, а также при получении дохода с таких операций, нет отдельного налогового режима для организаций, которые занимаются продажей, обменом и хранением цифровых прав и т. д. Налоговая служба дает разъяснения только по поводу дохода по ЦФА. Доход учитывается согласно п. 1 ст. 346 НК РФ по упрощенной системе налогообложения, а также в соответствии с п. 1 ст. 248 НК РФ доход от ЦФА будет относиться к доходу от реализации товаров (работ, услуг). Однако Налоговая служба не дает разъяснений, как будут учитываться сделки по утилитарным цифровым правам.

В связи с последними заявлениями Минфина Российской Федерации на своем официальном сайте от 14.04.2022 ведомство в своем законопроекте «О цифровой валюте» термин «квалифицированный инвестор» заменяет на «профессиональный приобретатель цифровой валюты». По сути, определение термина не меняется, изменяется только название.

По нашему мнению, благодаря замене термина будет устранено ошибочное отнесение квалифицированного инвестора по цифровым правам к инвестору по ценным бумагам. Данное изменение носит уточняющий характер и положительно может сказаться на сделках с цифровыми правами.

Профессиональным приобретателем, в соответствии с обновленной версией законопроекта, внесенного Минфином в Правительство РФ, является физическое лицо, признанное таковым оператором цифровой торговой платформы или оператором обмена цифровой валюты в порядке, установленном правительством. Тех, кто может стать профессиональным приобретателем, а также порядок становления таковым установит Правительство РФ после одобрения предложенных изменений.

По вопросам оборотоспособности цифровых прав Банк России на одном из заседаний принял решение получить от Правительства РФ решение для выдачи биржам лицензии на продажу цифровых финансовых активов. В случае получения разрешения от Правительства РФ и выдачи лицензии Банком России фондовые биржи проведут листинг финансовых активов, в том числе утилитарных прав, и смогут торговать ими на биржах.

С одной стороны, появление цифровых прав на бирже повысит их оборот в России. С другой – доступ для физических лиц не будет открыт на биржах, цифровые права смогут приобретать только юридические лица и, к примеру, брокеры (профессиональные приобретатели).

Следовательно, требуется после получения разрешения на торговлю цифровыми правами на бирже внести изменения в законодательство. Так, предлагается пересмотреть Закон о рынке ценных бумаг. Требуется внести изменения в гл. 2 данного закона, дополнить статьей о профессиональном приобретателе цифровых активов и его обязанностей. А также дополнить гл. 4 положениями об обращении цифровых активов на фондовой бирже.

Список литературы

1. Постановление от 3 июня 2020 г. по делу № А40–164942/2019. URL: https://sudact.ru/arbitral/doc/vUuWu4jiaxJB/? (дата обращения 10.09.2022)

2. Савельев А. И. Некоторые риски токенизации и блокчейнизации гражданско-правовых отношений // Закон. 2018. № 2. С. 7–14.

3. Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права. // Вестник гражданского права. 2016. Т. 16, № 3. С. 32–60.

4. Указание Банка России от 25.11.2020 № 5635-У «О признаках цифровых финансовых активов, приобретение которых может осуществляться только лицом, являющимся квалифицированным инвестором, о признаках цифровых финансовых активов, приобретение которых лицом, не являющимся квалифицированным инвестором, может осуществляться только в пределах установленной Банком России суммы денежных средств, передаваемых в их оплату, и совокупной стоимости иных цифровых финансовых активов, передаваемых в качестве встречного предоставления, об указанных сумме денежных средств и совокупной стоимости цифровых финансовых активов» // Министерство юстиции России. 2020. № 61622.

Ю. О. Лысаковская,
старший преподаватель кафедры хозяйственного права,
Белорусский государственный университет

АГЕНТИРОВАНИЕ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПЕРСПЕКТИВЫ РАЗВИТИЯ

Аннотация. Развитие искусственного интеллекта уже ставит вопрос перед правоведами о придании электронным агентам статуса агента юридического. Недавнее решение Федерального суда Австралии по делу Талера о признании искусственной нейронной сети DABUS автором изобретения демонстрирует возможный переворот в судебной практике в части того, что электронные агенты являются не только автоматическими, но и автономными. Автор анализирует перспективы наделения электронных агентов правосубъектностью и делает вывод о некорректности отнесения электронных агентов к юридической личности, субъекту правоотношений, на данном этапе развития технологий и права.

Ключевые слова: агент, искусственный агент, электронный агент, программный агент, правосубъектность, ответственность, искусственный интеллект, слабый искусственный интеллект, сильный искусственный интеллект, смарт-контракты, мудрые контракты, блокчейн

AGENCY AND ARTIFICIAL INTELLIGENCE: FUTURE AND PROSPECTS

Abstract. Based on the development of artificial intelligence legal scholars are already faced with the question whether or not electronic agents (or artificial agents) are legal agent. The recent decision of the Federal Court of Australia in the Thaler case recognizes the DABUS artificial neural network as an inventor, and it just illustrates a very possible reversal in the jurisprudence that electronic agents are not only automatic but also autonomous. The author analyzes the prospects of conferring legal personality on electronic agents and makes findings there are no grounds yet at this stage of development of technology and law to confer legal personality on electronic agents.

Keywords: Agency, Artificial agents, Electronic agents, Software agents, Legal personality, Liability, Artificial intelligence, Weak AI, Strong AI, Smart-contracts, Wise-contracts, Blockchain

Введение. В июле 2021 г. судья Федерального суда по делу Thaler v. Commissioner of Patents FCA 879 постановил, что искусственный интеллект (далее – ИИ) может быть указан автором изобретения при подаче заявки на регистрацию патента [9, 14]. В своем решении суд ссылался на статью 15 Закона о патентах 1990 г. (Patents Act 1990), в силу которой «те, кто вносит свой вклад или предоставляет изобретательскую концепцию, имеют право на получение гранта. Выдача патента на изобретение вознаграждает их изобретательность» [11].

Однако 13 апреля 2022 г. апелляционная инстанция Федерального суда по делу Commissioner of Patents v Thaler [2022] FCAFC 62 отменила решение суда первой инстанции и определила, что «изобретателем» в заявке о регистрации патента должно быть указано физическое лицо, обосновав свое решение комплексным

толкованием Закона о патентах, историей его принятия, а также статьей 3.2C(2)(aa) Патентной инструкции (Patents Regulations 1991) [9, 14].

Вместе с тем следует отметить, что Федеральный суд Австралии в своем решении рекомендовал законодателю рассмотреть возможные изменения в закон, например:

– Следует ли включатель в перечень правообладателей патента (изобретателя) искусственный интеллект?

– Если да, то кому следует выдать патент на изобретения, созданные ИИ: владельцу машины, на которой работает программное обеспечение искусственного интеллекта; владельцу авторских прав на его исходный код или человеку, который вводит данные, используемые искусственным интеллектом для разработки его выходных данных? [9].

Доктор Талер доказывал в судах ряда юрисдикций довод о том, что владелец систем искусственного интеллекта должен по умолчанию признаваться владельцем патентов на изобретения, созданные такими системами. Помимо этого, он утверждал, что указанные системы искусственного интеллекта следует определять в качестве изобретателя в патентных заявках [9, 14].

Позиция австралийского суда поддерживается позицией судов Великобритании, Европейского союза и США. Так, Апелляционный суд Лондона постановил, что системы искусственного интеллекта не могут владеть патентными правами или передавать их в соответствии с законодательством Великобритании, а изобретателем может быть только физическое лицо. Европейское патентное ведомство также отклонило аргументы доктора Талера в 2020 г., как и Окружной суд штата Вирджиния, США [9, 14].

Однако патентный орган ЮАР все же удовлетворил заявку доктора Талера. Справедливости ради следует отметить, что в ЮАР работает депозитарная система регистрации прав на объекты интеллектуальной собственности, что исключает официальное рассмотрение заявки [9, 14].

Приведенный пример – новый поворот в общемировых дебатах относительно необходимости изменения концептуальных подходов законодательств в целях адаптации к стремительно изменяющейся сфере инноваций.

Основная часть. Искусственный интеллект можно рассматривать в качестве некоего электронного агента лица, им владеющего. Развитие технологий, как мы рассмотрели выше, уже ставит вопрос перед правоведами о придании электронным агентам статуса агента юридического.

Так что же такое «электронный агент»? Практически каждый из нас сталкивается с ними ежедневно при использовании своих смартфонов, например приложения Siri (Apple), Alexa, Алиса (Яндекс), или автономных устройств, таких как «умные колонки», иных устройств дистанционного управления. По сути, электронный агент, или искусственный агент (программный агент) [7], – это часть новой экосистемы – интернета вещей [8].

Безусловно, использование электронных агентов в электронной коммерции может вызвать множество трудностей, особенно в отношении действительности агентских договоров и возложения ответственности за действия таких агентов.

В качестве наглядного примера работы электронного агента посредством смарт-контракта можно привести Uber и Яндекс.Такси. В данном случае агрегаторы выступают посредником (агентом водителя): потребитель выражает согласие оплатить поездку по цене, предложенной электронным агентом (агрегатором), а принципал – водитель обязуется оказать потребителю услугу по перевозке пассажиров (грузов) до заранее определенного места.

Возникает справедливый вопрос: каков правовой статус договора, заключенного через автоматизированную систему? Имеет ли договаривающаяся сторона в случае ошибки или сбоя, допущенных автоматизированной системой, право на судебную защиту в силу договора или в силу причинения вреда?

В соответствии с ч. 2 ст. 309 Гражданского кодекса Российской Федерации (далее – ГК РФ) [1] условия сделки могут предусматривать исполнение сторонами возникающих из нее обязательств при наступлении определенных обстоятельств без направленного на исполнение обязательства отдельно выраженного дополнительного волеизъявления сторон путем применения информационных технологий, определенных условиями сделки. Фактически российским законодателем легализована возможность исполнения сделок посредством смарт-контрактов (самоисполняемых сделок) в отсутствие легального определения смарт-контракта. Как следствие, отсутствие бумажного договора несет определенные риски в сфере налогообложения, бухгалтерского учета и отчетности, которые, как видится, можно нивелировать путем дублирования смарт-контракта договором на бумажном носителе или электронным документом, заверенным электронными цифровыми подписями.

Иначе обстоят дела в белорусской правовой системе. Революционный Декрет Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики» (далее – Декрет № 8) [3] в п. 9 приложения 1 к нему содержит дефиницию смарт-контракта как программного кода, предназначенного для функционирования в реестре блоков транзакций (блокчейне), иной распределенной информационной системе в целях автоматизированного совершения и (или) исполнения сделок либо совершения иных юридически значимых действий. Как следует из приведенного определения, смарт-контракт представляет собой техническое средство, а не сделку или ее форму. Лицо, совершившее дистанционную сделку с использованием смарт-контракта, считается надлежащим образом осведомленным о ее условиях, в том числе выраженных программным кодом. Оферта, направленная в виде кода, признается соблюдением требования пункта 2 ст. 402, п. 2 ст. 404 Гражданского кодекса Республики Беларусь (далее – ГК Республики Беларусь) о простой письменной форме сделки (п. 3 ст. 404 ГК Республики Беларусь) [2].

Вместе с тем право совершать и (или) исполнять сделки посредством смарт-контрактов предоставлено только нескольким категориям субъектов права: резидентам Парка высоких технологий в порядке правового эксперимента (пп. 5.3 п. 5 Декрета № 8) и участникам банковских и иных финансовых операций (ч. 1 пп. 1.13 п. 1, абзац 3 п. 4 Указа Президента Республики Беларусь от 18.04.2019 № 148 «О цифровых банковских технологиях» [4]).

Представляется все же обоснованным перенять опыт России и легализовать возможность совершения и исполнения сделок посредством смарт-контрактов, включив соответствующую норму в Гражданский кодекс Республики Беларусь.

Возвращаясь к вопросу правового статуса договора, заключенного через электронного агента, отметим, что автор разделяет позицию ряда исследователей, включая нобелевских лауреатов по экономике 2016 г. Оливера Харта и Бенгта Хольмстрема (Oliver Hart and Bengt Holmström), основанную на теории контрактов, что крайне важно, чтобы смарт-контракт представлял собой юридически обязательный договор, «умный» юридический договор [10]. Некоторые ученые предлагают перейти от «умных» к «мудрым» контрактам (wise contracts). Так, Джеймс Хазард и Хелена Хаапио определяют термин «смарт-контракт» как соглашение, которое исполняется автоматически либо принудительно, охватывая одновременно и «умный юридический договор» (smart legal contract), и «умный код контракта» (smart contract code), а также вводят термин «мудрый контракт» (wise contract). Под «мудростью» ученые подразумевают включение функций, позволяющих определять деловую (экономическую) и юридическую цели контракта и способы их достижения [10. С. 1].

Смарт-контракты используются для выполнения либо чисто «алгоритмических» вычислений (например, автоматизация комиссий или акций, обеспечение прав доступа и т. д.), либо интерактивных вычислений, направленных на определение того, когда, как и в какой степени лица, не входящие в цепочку поставок (продаж) отдельной компании могут коммуницировать [15]. Таким образом, интеграция системы коммерческого посредничества и блокчейна представляется многообещающей. Агенты, как коммерческие посредники, являются независимыми (автономными) субъектами по распределению товаров (работ, услуг), деятельность и взаимодействие которых подлежит должному регулированию со стороны принципала. В то же время блокчейн и смарт-контракты представляют собой trust-sensitive инструмент, приемлемый для управления взаимодействием принципал – агент – потребитель [6].

Например, производитель товара желает экспортировать свой товар за границу. Классическая схема будет выглядеть как цепочка поставок, включающая в себя транспортную компанию (грузоперевозчика), дистрибьюторскую компанию (агента) и розничный магазин (рис. 1).

Рис. 1. Традиционная цепочка сбыта товара (разработка автора)

А так будет выглядеть цепочка продвижения товара до конечного потребителя (в розничной торговле, например) с применением технологии блокчейн (рис. 2).

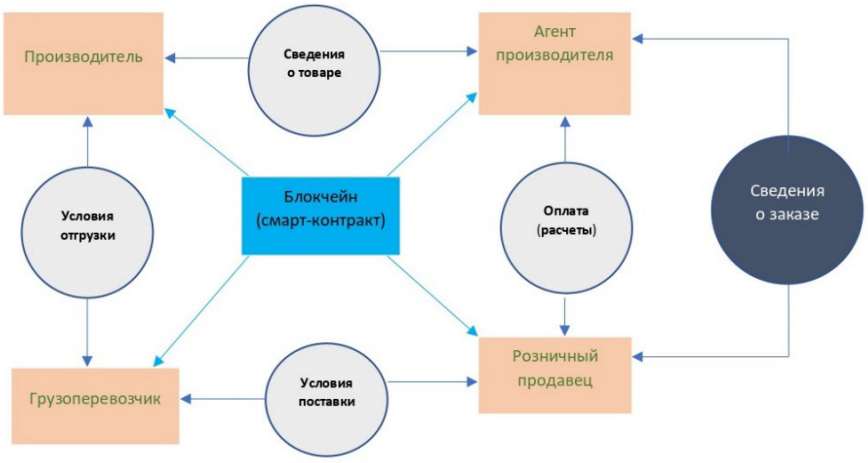

Рис. 2. Цепочка сбыта товара с применением технологии блокчейн (разработка автора)

Некоторые правоведы (как будет рассмотрено далее) утверждают, что указанные вопросы лучше всего разрешить, наделив автоматизированные системы правосубъектностью.

Полагаем, что стоит все же адаптировать данные процессы на основе именно деликтного права путем принятия различных стандартов ответственности в зависимости от того, выполняется ли действие автономно оставленным без присмотра программным обеспечением или это делается автоматически с помощью программного обеспечения.

В попытке создать искусственного агента, обладающего теми же свойствами, что и юридический агент (лицо, обладающее правосубъектностью), Рассел и Норвиг в своем исследовании фокусируются на том, делает ли искусственный агент «правильные вещи». Таким образом, выбор искусственным агентом того или иного действия всегда зависит от: а) его встроенных знаний и б) от последовательности содержания, воспринимаемой его датчиками (последовательность восприятия агента). В то время как люди имеют свои собственные желания и предпочтения, выбирают действия, которые дают им желаемый результат, с учетом этических, моральных и юридических норм, машины (не имеющие собственных желаний и предпочтений) запрограммированы максимизировать свою производительность, т. е. проявляют свои «рациональность» (rationality) и «интеллект» (intelligence) [12. С. 36–39].

Сторонники теории о признании искусственных агентов (artificial agents) субъектами агентских правоотношений наравне с агентом – физическим или юридическим лицом аргументируют свою позицию тем, что электронные агенты: а) «обладают интеллектом» и б) «свободой действий» [5]. Приверженцы данной теории признают пользователей таких электронных агентов принципалами в понимании субъекта агентских правоотношений. Так, профессор Самир Чопра утверждает, что «компьютерные программы – тоже люди» и «релевантной в дан-

ном случае является концепция полномочий, содержащаяся в законодательстве об агентском договоре, которое ограничивает полномочия агента принимать решения от имени принципала. Существование такого ограничения предполагает дискреционное право принимать решения, которые не были бы приняты самим принципалом. Таким образом, на первый взгляд, искусственные агенты, заключающие контракты от имени корпораций или пользователей, которые их используют, функционируют как юридические личности» [5. С. 34].

То есть данная теория утверждает, что юридическому агенту не требуется полная правоспособность: агенту не требуется способность иметь законные права или нести ответственность по обязательствам принципала по аналогии с правоспособностью ребенка [5. С. 41–42]. Поскольку в системе общего права (common law) ребенок имеет право заключать договоры, связывающие его мать или опекуна, даже если мать не обладает правоспособностью связать себя договором, так и искусственные агенты могут выступать в качестве юридических агентов, связывающих своих принципалов – субъектов правоотношений. Рассматриваемая теория также признает судна и компании искусственными юридическими личностями, обладающими правоспособностью, имеющими права и несущими обязательства [5. С. 379].

Автор разделяет мнение противников данной теории, например Дэниела Сенга и Тана Ченга Хана [13], о ее дефектности, так как в отличие от электронных агентов, люди, так же как и компании, лежат в основе деятельности судов и компаний.

Заключение. Посредничество присуще многим сферам хозяйственной деятельности, особенно в сфере коммерции. Все чаще такие субъекты агентских правоотношений, как корпорации, заключают сделки не через посредников (лиц юридических или физических), а с помощью искусственных агентов.

Вместе с тем полагаем, что искусственных агентов преждевременно наделять правосубъектностью до тех пор, пока технологии искусственного интеллекта не создадут искусственного агента с необходимым и достаточным уровнем рациональности и интеллекта. Но даже если искусственные агенты достигнут разумности и осознанности, они не могут быть агентами де-юре, если только не будут признаны субъектами агентских правоотношений.

Вне зависимости от того, насколько сложна часть кода, код не может быть агентом де-юре в отсутствие легального определения его как юридической личности и выработки механизма практической реализуемости привлечения к ответственности искусственного агента. Например, корпорации как юридические лица обязаны раскрывать информацию о своем состоянии посредством проведения ежегодного аудита. По аналогии, в случае с искусственным интеллектом компании-агенты должны быть обязаны раскрывать условия агентских договоров и их функциональных возможностей и др.

Таким образом, развитие информационных технологий неизбежно проникает во все сферы общественных отношений. Применение смарт-контрактов в случае с коммерческим посредничеством (агентированием, дистрибьюторством), в том числе посредством электронных агентов, технически уже возможно и применимо.

Вместе с тем вопросы правового регулирования отношений сторон смарт-контрактов до настоящего времени остаются открытыми:

– отсутствует правовое регулирования смарт-контрактов в национальных правовых системах и международном праве;

– вопросы определения применимого права (материального и процессуального);

– исполнимость вынесенного решения в трансграничных отношениях и на территории страны местонахождения виновной стороны;

– отсутствие судебной практики.

В научном сообществе предлагается перейти от «умных» контрактов к «мудрым» (wise contracts), которые должны быть понятны, технологичны и законны. Возможно, «мудрые» контракты смогут восполнить существующие пробелы.

Представляется, что для развития применимости смарт-контрактов в деловом обороте России и Беларуси требуется легально определить правовой статус самого смарт-контракта и его сторон, механизм защиты прав и интересов каждой из сторон и выработать единообразный подход к применению соответствующих норм.

Существующие на сегодняшний день электронные агенты все еще остаются примерами так называемого слабого искусственного интеллекта (Weak AI) и, как нам видится, все же не имеют подлинной автономии, а значит, и не могут обладать правосубъектностью.

Кроме того, квалификация электронных агентов в качестве субъектов права не является необходимой, поскольку их действия (и злоупотребления) могут быть юридически урегулированы на основе общих принципов деликтной ответственности и механизма ее реализации, аналогично тому, как определяются основания возникновения обязательств вследствие причинения вреда у владельца источника повышенной опасности (ст. 1070 ГК РФ, ст. 948 ГК Республики Беларусь).

В случае признания электронных агентов инструментом принципала – лица в терминологии гражданского законодательства, вопросы привлечения к ответственности электронных агентов вполне себе разрешимы на основе договорного и деликтного права. Полагаем, что до тех пор, пока не будут созданы системы «сильного искусственного интеллекта» (Strong AI), вопрос о правосубъектности электронных агентов не должен сдерживать развитие технологий и права в сфере искусственного интеллекта.

Список литературы

1. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 01.07.2021, с изм. от 08.07.2021) (с изм. и доп., вступ. в силу с 01.01.2022) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_9027/27fb9de9d0fa6adb1f00e22c245b99251d5bd23f/ (дата обращения: 15.09.2022).

2. Кодекс Республики Беларусь от 07.12.1998 № 218-З (ред. от 18.07.2022) «Гражданский кодекс Республики Беларусь» // СПС Ilex. URL: https://ilex-private.ilex.by/view-document/BELAW/197814/%D0%B8%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%20%D0%BF%D0%BE%D0%B2%D1%8B%D1%88%D0%B5%D0%BD%D0%BD%D0%BE%D0%B9?searchKey=sq63#M100001 (дата обращения: 15.09.2022).

3. Декрет Президента Республики Беларусь от 21.12.2017 № 8 (ред. от 18.03.2021) «О развитии цифровой экономики» // СПС Ilex. URL: https://economy.gov.by/uploads/files/sanacija-i-bankrotstvo/Dekret-Prezidenta-Respubliki-Belarus-ot-21–12–2017-N-8-O-r.pdf (дата обращения: 15.09.2022).

4. Указ Президента Республики Беларусь от 18.04.2019 № 148 «О цифровых банковских технологиях» // СПС Ilex. URL: https://ilex-private.ilex.by/view document/BELAW/181194/?searchKey=j1wx#M100068 (дата обращения: 15.09.2022).

5. Chopra S., White L. F. A legal theory for autonomous artificial agents. The University of Michigan Press, 2011. 264 p.

6. Ciatto G., Mariani S., Maffi A., Omicini A. Blockchain-based coordination: Assessing the expressive power of smart contracts // Information. 2020. № 11 (1). DOI: 10.3390/info11010052

7. Dahiyat E. A. R. Law and software agents: Are they “Agents” by the way? // Artif Intell Law. 2021. № 29. URL: https://doi.org/10.1007/s10506–020–09265–1 (дата обращения: 12.09.2022).

8. Gillis A. S. What is the internet of things (IoT)? URL: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (дата обращения: 12.09.2022).

9. Grierson L. Court of the Federal Court of Australia dismisses DABUS – An AI system cannot be an Inventor // Gadens. 2022. May 11. URL: https://www.gadens.com/legal-insights/full-court-of-the-federal-court-of-australia-dismisses-dabus-an-ai-system-cannot-be-an-inventor/ (дата обращения: 12.09.2022).

10. Hazard J., Haapio H. Wise contracts: smart contracts that work for people and machines // Conference: International Legal Informatics Symposium IRIS 2017. February 2017. Salzburg, Vienna. URL: https://www.researchgate.net/publication/314263820_Wise_Contracts_Smart_Contracts_that_Work_for_People_and_Machines/stats (дата обращения: 15.09.2022).

11. Patents act 1990 of Commonwealth of Australia. № 83, 1990 (amended as Act № 9, 2020, Act № 154, 2020). URL: http://www5.austlii.edu.au/au/legis/cth/consol_act/pa1990109/notes.html (дата обращения: 12.09.2022).

12. Russell S., Norvig P. Artificial Intelligence: A Modern Approach (Pearson Series in Artifical Intelligence). 4th ed. 2021.

13. Seng D. K. B., Tan C. H. Artificial Intelligence and Agents // NUS Centre for Technology, Robotics, Artificial Intelligence & the Law Working Paper 21/02. NUS Law Working Paper № 2021/019. July 20, 2021. City University of Hong Kong School of Law Legal Studies Research Paper No. Forthcoming. DOI: http://dx.doi.org/10.2139/ssrn.3935446

14. Vincent J. AI systems can’t patent inventions, US federal circuit court confirms // The Verge. 2022. August 8. URL: https://www.theverge.com/2022/8/8/23293353/ai-patent-legal-status-us-federal-circuit-court-rules-thaler-dabus (дата обращения: 12.09.2022).

15. Wegner P. Why interaction is more powerful than algorithms // Commun. ACM. May 1997. № 40, 5. Pp. 80–91. DOI: 10.1145/253769.253801

С. А. Минич,
младший научный сотрудник,
Национальный центр законодательства и правовых исследований
Республики Беларусь

О СОВЕРШЕНСТВОВАНИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРЕДПРИНИМАТЕЛЬСКОЙ И ИНОЙ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭКОНОМИКИ

Аннотация. В статье рассматриваются проблемные правовые аспекты, обусловленные новой цифровой реальностью, с которыми столкнулось предпринимательское сообщество, а также пути их решения. Стремительное развитие цифровых технологий привело к образованию большого количества нецелесообразных, «спящих» регуляторных норм, не отвечающих требованиям и принципам рыночной экономики, что стало причиной возникновения непреодолимых препятствий для ведения бизнеса и излишней административной нагрузки, послужило основанием для поиска новых эффективных законодательных механизмов по устранению избыточного правового регулирования. Значительную роль в решении вопросов по сокращению обременительных регуляций и обеспечению правовой устойчивости в условиях цифровой трансформации экономики играет активное внедрение механизмов дерегулирования, одним из которых выступает «регуляторная гильотина». Автор анализирует опыт ряда стран по внедрению «регуляторной гильотины» с целью актуализации законодательства и совершенствования системы регулирования бизнеса путем быстрого, масштабного пересмотра и отмены устаревших, неработающих правовых норм, а также сохранения и корректировки действующих правил при их соответствии установленным критериям надлежащего регулирования. Использование кардинально нового механизма оптимизации нормативного массива в сфере предпринимательства потребовало серьезной поэтапной работы по созданию надлежащей правовой основы для успешной его реализации.

Ключевые слова: цифровая трансформация, дерегулирование, регуляторная гильотина, предпринимательская деятельность, избыточность нормативного массива

ON IMPROVING THE LEGAL REGULATION OF ENTREPRENEURIAL AND OTHER ECONOMIC ACTIVITIES IN THE CONTEXT OF THE DIGITAL TRANSFORMATION OF THE ECONOMY

Abstract. The article examines the problematic legal aspects caused by the new digital reality that the business community has faced, as well as ways to solve them. The rapid development of digital technologies has led to the formation of a large number of inappropriate, “dormant” regulatory norms that do not meet the requirements and principles of a market economy, which caused insurmountable obstacles to doing business and excessive administrative burden, served as the basis for the search for new effective legislative mechanisms to eliminate excessive legal regulation. A significant role in solving

issues of reducing burdensome regulations and ensuring legal stability in the context of digital transformation of the economy is played by the active introduction of deregulation mechanisms, one of which is the “regulatory guillotine”. The author analyzes the experience of a number of countries in implementing the “regulatory guillotine” in order to update legislation and improve the business regulation system through a rapid, large-scale revision and cancellation of outdated, non-working legal norms, as well as maintaining and adjusting existing rules in accordance with the established criteria for proper regulation. The use of a radically new mechanism for optimizing the regulatory array in the field of entrepreneurship required serious step-by-step work to create an appropriate legal framework for its successful implementation.

Keywords: Digital transformation, Deregulation, Regulatory guillotine, Entrepreneurial activity, Redundancy of the regulatory array

Введение. В условиях перехода к новой технологической и инновационной реальности, глобальных цифровых трансформаций процесс поддержания действующего законодательства в актуальном состоянии – достаточно сложная задача, обусловленная опасностью появления как пробелов в правовом поле, так и чрезмерного регулирования, что мешает развитию бизнеса. Многие нормы и правила по объективным причинам устаревают, приобретают формальный и избыточный характер. Привычные правовые механизмы зачастую не всегда могут оперативно справиться с возрастающим объемом избыточных требований к бизнесу, что служит основанием для поиска действенных регуляторных технологий в целях упорядочения и оптимизации нормативного массива. Одной из форм избавления от обременительных правил является дерегулирование, включающее в себя различные правовые средства для быстрого анализа и пересмотра большого количества требований, предъявляемых к субъектам предпринимательства. Среди наиболее передовых инструментов дерегулирования выступает «регуляторная гильотина». Успешный опыт ряда стран по пересмотру действующих нормативных правовых актов, устанавливающих обязательные требования, связанные с предпринимательской деятельностью, позволил в ходе проведения широкомасштабных и более узких реформ на основе «регуляторной гильотины» отменить все требования, которые не прошли фильтрацию, т. е. были признаны устаревшими, тормозящими, неработающими, что значительно сократило риски и регулятивные издержки для бизнеса.

Вопросам совершенствования правового регулирования предпринимательской деятельности путем активного внедрения механизмов дерегулирования в условиях цифрового преобразования экономики посвящены научные работы целого ряда ученых: О. В. Александрова; Ю. Г. Арзамасова, Р. Ю. Березнева, А. А. Венедиктова; А. В. Войтюля, А. Е. Голодникова, А. А. Ефремова, М. В. Дегтярева, А. Б. Дидикина, Е. А. Дмитриева, А. В. Мартынова; В. М. Минько, О. Н. Русак, И. В. Сехина, Ю. А. Тихомирова, Д. Б. Цыганкова, В. Н. Южакова и др.

Основная часть. Несмотря на значительное количество исследовательских работ, раскрывающих различные вопросы цифровизации, до сих пор нет однозначного устойчивого понимания сущности и содержания термина «цифровая трансформация», что вполне объяснимо. Определение данного понятия эволюци-

онирует вместе с изменением и развитием цифровых технологий, приобретая все более многогранный характер. Цифровая трансформация, проникнув абсолютно во все сферы деятельности, быстрыми темпами меняет нашу действительность. Что касается экономики, то тут, в первую очередь, необходимо указать на особую масштабность рассматриваемого процесса. Цифровая экономика открыла широкие возможности для интеграции в систему мирохозяйственных связей, способствовала продвижению новых высокоэффективных форм развития бизнеса, выступила своего рода серьезным стимулом экономического роста и базисом для прорывных инноваций.

Успешное внедрение цифровых технологий невозможно без конструктивного диалога государства и бизнеса в интересах общества и экономической безопасности страны путем обеспечения предсказуемо-адекватного правового регулирования экономических отношений без завышенных требований, как для субъектов предпринимательской деятельности, так и для самого государства, отвечающего принципам рыночной экономики, стремящегося действовать на опережение. Однако, несмотря на все усилия большинства стран по сохранению правовой стабильности, переход к цифровой экономике стал одной из причин возникновения определенных сложностей в регулировании общественных отношений в данной сфере. В частности, бизнес-сообщество столкнулось с проблемой зарегулированности экономического поведения и неоправданных административных барьеров со стороны государственных органов. Огромное количество обязательных требований, установленных положениями действующих нормативных правовых актов, уже устарело и не отвечало современным потребностям субъектов экономической деятельности, уровню развития науки и технологий, содержанию новых экономических отношений, и создавало определенные препятствия в регулировании, нарушая его стабильность. Все это привело к появлению серьезной проблемы избыточности нормативного массива – ситуации, когда невозможно в ходе осуществления предпринимательской деятельности соблюсти все обязательные требования, так как адресаты правовых норм, содержащих обязательные требования, вынуждены постоянно усваивать стремительно увеличивающийся объем правовой информации, связанной с появлением все новых и новых нормативных правовых актов и отдельных правил, следить за бесконечной новеллизацией действующего законодательства и приспосабливаться к его постоянному изменению и усложнению всей системы правового регулирования. Сложившиеся трудности в регулировании потребовали проведения активной работы по оптимизации и гармонизации законодательства в данной сфере, внедрению новейших регуляторных технологий с целью ретроспективной оценки действующих нормативных правовых актов, содержащих требования к ведению бизнеса. Среди наиболее прорывных и часто используемых механизмов дерегулирования можно выделить «регуляторную гильотину», принцип работы которой был использован рядом зарубежных стран при широкомасштабном пересмотре всех требований, утративших свою актуальность и мешающих экономическому росту.

Цель регуляторной гильотины – формирование эффективной системы актуальных, понятных и четких обязательных требований к субъектам предпри-

нимательства путем прекращения действия устаревших правил в пользу бизнеса. Данный механизм применяется при необходимости быстрого, комплексного пересмотра и актуализации законодательства. Концепт регуляторной гильотины основан на позиции относительно того, что проблема регулирования предпринимательской деятельности является системной по своему характеру [1. С. 86].

Суть регуляторной гильотины достаточно проста. Данный механизм означает выбор, утверждение, изменение или отмену действующих нормативных правовых актов посредством их анализа или пересмотра. Реализуется это пакетировано, т. е. без использования продолжительных и ресурсозатратных процедур в отношении каждой регуляции [1. С. 86].

Метод регуляторной гильотины, как утверждают Три Тхань Во и Куонг Ван Нгуен, стал популярен именно в силу возможности получения с ним достаточно быстрых результатов за счет сокращения и упрощения «ненужных» норм [3. С. 19]. Более того, данная регуляторная технология активно используется для преодоления барьеров, замедлявших или блокировавших проведение широкомасштабных правовых реформ ранее (к таким барьерам могут, к примеру, быть отнесены существенные политические и административные издержки, а также значительная внутренняя системная резистентность к изменениям) [2. С. 87].

Ведран Антоляк, Домагой Юричич и Марко Слуньски отмечают, что регуляторные гильотины используются для целей создания баз данных и официальных реестров правовой информации [2. С. 86].

Новатором среди стран СНГ по внедрению механизма регуляторной гильотины для быстрого пересмотра нормативной правовой базы в определенных секторах экономики и устранения избыточных регуляций, выступила Республика Армения (далее – Армения), запустившая в ноябре 2011 г. по инициативе и при поддержке Ереванского бюро ОБСЕ проект «Регулирующая гильотина». Следует отметить, что к моменту запуска гильотины Армения не имела полноценной институциональной структуры оценки регулирующего воздействия (далее – ОРВ) и соответствующего опыта и методологии применения политики ОРВ. Принятые нормы по ОРВ не были апробированы и адаптированы на практике. Анализ воздействия нормативных правовых актов на ту или иную сферу экономической деятельности субъектов рынка проводился неэффективно [4]. Сложившаяся ситуация привела к появлению большого количества сложных и противоречивых нормативных правовых актов (около 25 000 законов и подзаконных актов), низкое качество которых ухудшало регулирование бизнеса и увеличивало уровень коррупции.

В поисках действенных мер по совершенствованию регулирования Армения приступила к реализации проекта «Регулирующая гильотина», цель которого – продвижение надлежащего экономического управления с помощью механизма ускоренного упрощения регуляций. Предметное поле охвата регуляторной реформой в Армении было определено широко. Требовалось пересмотреть законодательство в 17 сферах (Указ Президента Республики Армения от 17 сентября 2011 г. № УП-246-Н).

Реализация проекта осуществлялась специально созданным для проведения регуляторной реформы Национальным центром по урегулированию законодатель-

ства (далее – НЦУЗ), утвержденным Правительством Республики Армения 13 октября 2011 г., который был подотчетен Совету по реформам. Центр рассматривал нормативную правовую базу конкретных секторов экономики, занимался пересмотром и упрощением правовых норм, влияющих на экономическую активность и на повседневную жизнь людей. Рекомендации, разработанные НЦУЗ, в виде законопроектов сначала одобрялись Советом по реформам во главе с премьер-министром Армении, а затем – Правительством или Парламентом, в зависимости от типа документа.

Проект «Регулирующая гильотина» состоял из нескольких этапов, первый из которых был проведен в 2011–2013 гг. За 2013 г. анализу было подвергнуто 6 тыс. актов различного уровня [2]. Согласно рейтингу «Doing Business-2012» Армения за год продвинулась на 6 пунктов, заняв 55 позицию среди 183 стран, опередив в том числе Российскую Федерацию (120 позиция) и Республику Беларусь (69 позиция). В целом за 4 года действия «гильотины» правительство приняло 170 актов, из которых 120 – в 2014–2015 гг. В результате сократились расходы, обусловленные этими актами, и из 6,71 млрд драмов было сэкономлено 4,66 млрд драмов [5].

Армянский проект «Регулирующая Гильотина» был призван сократить регулятивные издержки в рассматриваемых секторах экономики на 50 %. Однако полученный результат показал снижение более чем на 60 %. При этом на реализацию «гильотины» было выделено около 1,1 млрд драмов, а сэкономить получилось в 4 раза, что говорит о 420 % эффективности проведенной реформы [6].

Несмотря на высокую результативность использования регуляторной гильотины при проведении реформы законодательства Армении, она имела разовый, бессистемный характер. Такое положение дел зачастую приводит к повторению проблемной ситуации в регулировании, так как законодательство с течением времени имеет тенденцию к росту, и Армения, как и любая другая страна, нуждается в периодическом пересмотре и «очищении» своей нормативной правовой базы.

Наибольший интерес среди стран СНГ по созданию эффективной системы установления и оценки применения обязательных требований, включающей в том числе механизм дерегулирования – «регуляторную гильотину», представляет изучение правового опыта Российской Федерации (далее – РФ). Процесс запуска и реализации комплексной регуляторной реформы в РФ был непростым, потребовав огромной работы со стороны государства. Особую значимость для формирования оптимальных условий взаимодействия бизнеса и государства, повышения качества регуляторных решений, наряду с уже существующими в РФ юридическими технологиями и аналитическими инструментами, имело внедрение и развитие таких институтов права, как оценка регулирующего воздействия (ОРВ) и оценка фактического воздействия (ОФВ), благодаря которым на новый уровень вышли процессы проектирования нормативных правовых актов и прогнозирования правовых последствий их принятия.

Предварительная (прогнозная, ex-ante) оценка регулирующего воздействия нормативных правовых актов, позволяющая эффективно блокировать принятие решений, подготовленных без достаточной проработки и прогноза возможных последствий введения нового регулирования, осуществляется во всех странах СНГ.

Оценка воздействия уже действующих нормативных правовых актов (ex post), направленная на пересмотр малоэффективных нормативных правовых актов в целях совершенствования регулирования в контексте исключения необоснованных обязанностей, запретов и ограничений для бизнеса, проводится в РФ, Кыргызской Республике и Республике Узбекистан. В Республике Казахстан в рамках анализа регуляторного воздействия осуществляется пересмотр действующих регуляторных инструментов и (или) требований, в отношении которых ранее не проводился анализ регуляторного воздействия. Однако точечный пересмотр нормативных правовых актов в ручном режиме не может противостоять активному разрастанию нормативного массива в условиях стремительно развивающихся экономических отношений. В связи с чем особое внимание было обращено на проведение комплексной, всесторонней ОРВ в виде единой процедуры, включающей ретроспективную оценку уже принятых нормативных правовых актов и использование отдельных новейших регуляторных технологий.

Комплексно к решению данного вопроса среди стран СНГ подошла именно РФ, уделив особое внимание проведению на регулярной основе всестороннего и прозрачного пересмотра всех действующих нормативных правовых актов во избежание всевозможных рисков, обусловленных в том числе процессами цифровой трансформации экономики.

Правительство РФ пришло к выводу, что без перехода к полному циклу ОРВ, включающего в себя проведение качественной ретроспективной расчистки нормативного поля, невозможно избежать определенных сложностей в регулировании предпринимательской деятельности, так как государственная машина постоянно вводит новые требования к бизнесу, которые с течением времени могут утрачивать свою актуальность, дублироваться, противоречить друг другу, создавая законодательные завалы, приводя к избыточному регулированию и неоправданным расходам со стороны бизнеса. Несмотря на видимую пользу и большой потенциал ОРВ, ОФВ и правового мониторинга, данные юридические технологии, даже в своей совокупности без включения в единую процедуру, на сегодняшний день не могут обеспечить пересмотр всех обязательных требований, в особенности в части устаревших регуляций, что, в свою очередь, создает предпосылки для внедрения новых инновационных регуляторных технологий оценки и оптимизации действующего законодательства (при сохранении и улучшении работы уже реализуемых механизмов оценки), позволяющих эффективно препятствовать необоснованному разрастанию нормативного поля. Кроме того, широкое использование целого спектра аналитических инструментов, сегодня стало своего рода трендом, актуальной практикой реформирования законодательства во многих государствах мира [2. С. 85]. Это объясняется в том числе их стремлением к формированию интегрированной регуляторной политики, объединяющей в себе различного рода регуляторные механизмы и технологии в единое целое для успешной систематизации, оптимизации и алгоритмизации всего нормативного массива и достижения стабильности в регулировании общественных отношений, складывающихся в результате осуществления предпринимательской и иной экономической деятельности.

Таким образом, РФ, делая шаг за шагом на пути к построению оптимальной системы обязательных требований, постепенно приближалась к решению о применении кардинальных мер для улучшения регулирования предпринимательской деятельности путем внедрения такой регуляторной технологий, как «регуляторная гильотина», которая может использоваться не только для узкой корректировки законодательства (по отдельным отраслям (подотраслям) экономики), но и для проведения широкомасштабных реформ, имеющих разовый или системный характер. Такой подход предусматривал полное вытеснение всего старого массива обязательных требований, не соответствующих темпам развития цифровой экономики. Поэтапному внедрению такой принципиально новой концепции «регуляторной гильотины» способствовало принятие целого ряда правовых актов: Плана мероприятий («дорожная карта») по реализации механизма «регуляторной гильотины, Методики исполнения плана мероприятий («Дорожной карты») по реализации механизма «регуляторной гильотины. Кроме того, в 2020 г. были приняты Федеральный закон «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» и Федеральный закон «Об обязательных требованиях в Российской Федерации» (далее – Закон № 247-ФЗ).

Закон № 247-ФЗ выступил системообразующим нормативным правовым актом, направленным на совершенствование правового регулирования предпринимательской деятельности в условиях стремительного развития цифровых технологий и лег в основу формирования нового для РФ правового института обязательного требования. Данный нормативный правовой акт обеспечил закрепление на законодательном уровне механизма «регуляторной гильотины» и включил в себя правила его реализации, что позволило быстро провести масштабный анализ и пересмотр действующих нормативных правовых актов во всех секторах экономики.

Опыт РФ по совершенствованию регулирования общественных отношений, возникающих при осуществлении предпринимательской деятельности, путем внедрения правового института обязательного требования, включающего механизм дерегулирования – «регуляторная гильотина», и направленного на формирование единых организационно-правовых основ установления и оценки применения обязательных требований, безусловно, вызывает интерес у многих стран и требует активного пересмотра устоявшихся подходов к регулированию, а также всестороннего изучения новых тенденций в правоприменительной практике.

Заключение. Переход к новой цифровой реальности, помимо очевидных благ, влечет за собой ряд проблемных правовых аспектов, с которыми сталкивается предпринимательское сообщество. В рамках данного исследования рассмотрению подлежал один из них, связанный с растущим количеством неэффективных, устаревших нормативных правовых актов, регламентирующих общественные отношения, возникающие в результате осуществления предпринимательской деятельности. Нормативная избыточность и чрезмерная зарегулированность экономического поведения стала проблемой, затронувшей многие страны, и предопределила необходимость появления инновационных правовых регуляторов. Законодательная инфляция, в частности, потребовала проведения активной работы по внедрению механизмов дерегулирования и сокращения числа требований, утративших свою

актуальность. Всестороннее изучение передовых практик по внедрению новейших регуляторных технологий, институтов регулирования и инструментов инвентаризации и систематизации законодательства позволило отметить успешный опыт ряда стран в реализации стратегии «регуляторной гильотины».

Список литературы

1. Дегтярев М. В. Новейшие регуляторные технологии и инструменты: Регуляторные эксперименты, песочницы, гильотины, экосистемы, платформы / под ред. д.ю.н., проф. И. В. Понкина / МГЮА. – М.: Буки Веди, 2022. – 424 с.

2. Зембатов М. Р. Развитие системы оценки регулирующего воздействия в Республике Армения // Науч.-исслед. финанс. ин-т. Финансовый журнал. 2018. – № 6 (46). С. 120–127.

3. Новые подходы к регуляторной реформе. URL: https://regulatoryreform.com/услуги/ (дата обращения: 14.09.2022).

4. Погосян А. Т. Проблемы становления системы оценки регулирующего воздействия правовых актов на экономику в Армении // Сектор экономики знаний Южного макрорегиона: институциональные инновации, технологии контроллинга, управления знаниями, развития человеческого капитала: Материалы IV Междунар. науч.-практ. конф., Краснодар, 28–30 сент. 2012 г. / отв. ред. В. В. Ермоленко, М. Р. Закарян. – Краснодар: Кубанский гос. ун-т, 2012. С. 80–86.

5. Программа «Регулирующая гильотина» сократит расходы бизнеса на $40 млн. URL: https://panarmenian.net/rus/news/195711 (дата обращения: 14.09.2022).

6. Сорокин А. Предложенные «Гильотиной» рекомендации привели к снижению затрат более чем на 60 %. URL: https://banks.am/ru/news/interviews/9437 (дата обращения: 14.09.2022).

Е. А. Мичурина,
кандидат юридических наук, доцент,
Саратовская государственная юридическая академия

К ВОПРОСУ О ПРАВОВОМ РЕГУЛИРОВАНИИ ЦИФРОВИЗАЦИИ ЭНЕРГЕТИКИ

Аннотация. С появлением в гражданском законодательстве цифровых прав актуализируются вопросы правового регулирования цифровизации экономики. В соответствии с требованиями объективной действительности область энергоснабжения нуждается во внедрении цифровых процессов, которые должны иметь правовые основания. Однако до настоящего времени нормативно-правовая база цифровых прав в области энергетики не является устойчивой и не представляется унифицированной. В статье автор анализирует основные подходы в правовом регулировании цифровизации энергетики, обозначает основные ее направления, выявляет проблемы и предлагает пути их решения.

Ключевые слова: право, цифровые технологии, цифровизация энергетики, энергоснабжение, энергетический комплекс, цифровая экономика, энергоэффективность

ON THE ISSUE OF LEGAL REGULATION OF DIGITALIZATION OF ENERGY

Abstract. With the advent of digital rights in civil legislation, the issues of legal regulation of the digitalization of the economy are being updated. In accordance with the requirements of objective reality, the field of energy supply needs the introduction of digital processes that must have legal grounds. However, to date, the regulatory framework of digital rights in the field of energy is not sustainable and does not seem unified. In the article, the author analyzes the main approaches in the legal regulation of the digitalization of energy, identifies its main directions, identifies problems and suggests ways to solve such problems.

Keywords: Law, Digital technologies, Digitalization of energy, Energy supply, Energy complex, Digital economy, Energy efficiency

В условиях современного общества велико влияние процессов цифровизации на все отрасли экономики. Промышленность, в том числе энергетическая, не является исключением. Цифровизация промышленности предполагает создание цифрового пространства, которое призвано интегрировать производственные процессы, процессы обеспечения деятельности и безопасности предприятия, различное оборудование, призванное оптимизировать работу конкретного объекта путем программного управления и взаимодействия, с минимальным вмешательством человека или без такового. Цифровизация в промышленности ставит перед собой задачу сокращения временных затрат на принятие производственных решений, автоматизацию ряда процессов технического и организационного характера, увеличение производительности. Представляется, что энергетическая промышленность является стратегическим элементом инфраструктуры и содержания общества.

Длящийся период энергоперехода – самая значительная технологическая трансформация последнего столетия. Можно с уверенностью говорить о четвертой промышленной революции, набирающей обороты за счет внедрения киберфизических систем, что приводит к модернизации традиционных инфраструктурных отраслей.

В условиях структурного изменения энергетической отрасли трендом становится отказ предприятий энергетического сектора от создания масштабной инфраструктуры. Представляется, что основой цифровизации в сфере энергетики должны стать широкая автоматизация, продвинутая аналитика в сфере установления стоимости, технологии децентрализованной генерации энергии. Внедрение подобных технологий перспективно направлено на обеспечение целевых показателей энергии и повышение качества оказываемых услуг. Цифровизация становится тождественна конкурентоспособности и открывает доступ к рынкам будущего [7. С. 225].

Существующий международный опыт внедрения цифровых технологий иллюстрирует, что внедрение таких технологий на этапах добычи и переработки нефти и газа позволяет повысить эффективность технического обслуживания

оборудования, снизить внеплановые простои оборудования, увеличить показатели добычи нефти с одновременным снижением ее себестоимости [6. С. 89].

Сегодня цифровизация энергетики имеет ключевое значение для повышения результативности российской экономики. Основной задачей цифровизации в таком случае становится увеличение показателей энергоэффективности, надежности и безопасности энергосистем, а также снижение издержек.

Краткосрочные прогнозы говорят об увеличении доходов отраслевых компаний. И основной рост доходов должен достигаться за счет использования неанализируемых в настоящее время данных, автоматизации процессов и активного внедрения цифровых решений. Долгосрочная перспектива предполагает объединение цифровых продуктов в энергетической отрасли с решениями других отраслей [4. С. 68].

Сфера энергетики представляется структурно сложной и многоаспектной, что обуславливает неоднородность процессов цифровизации. Однако было бы неверным говорить об изменении энергетической отрасли, оперируя только технологическими данными и рассматривая процессы только с точки зрения применения решений. На наш взгляд, отправной точкой в модернизации энергетики, применении новых решений, позволяющих цифровую трансформацию, должны быть правовые механизмы. Логичное и достаточное правовое регулирование призвано ускорить энергопереход с внедрением цифровых продуктов с одновременным достижением перспективных целей.

Цифровизация энергетики является составной частью масштабного проекта по реализации цифровой экономики на территории Российской Федерации. Правовой основой для формирования национальной цифровой экономики являются Конституция Российской Федерации, Федеральный закон «О стратегическом планировании в РФ» от 28 июня 2014 г. № 172-ФЗ, Стратегия развития информационного общества в РФ на 2017–2030 гг., утвержденная Указом Президента Российской Федерации от 9 мая 2017 г. № 203, Указ Президента Российской Федерации от 21 июля 2020 г. № 474 «О национальных целях развития РФ на период до 2030 года», Стратегия национальной безопасности РФ, утвержденная Указом Президента РФ от 2 июля 2021 г. № 400, Указ Президента Российской Федерации от 10 октября 2021 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 321 «Об утверждении государственной программы Российской Федерации «Развитие энергетики» и ряд других актов.

В рамках институционального развития программы Указом Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития РФ на период до 2024 года» определена необходимость разработки и модернизации национальных проектов и программ в области энергетики, включая энергетическую инфраструктуру, посредством внедрения цифровых технологий и платформенных решений.

Однако до настоящего времени содержание нормативно-правовой и нормативно-технической баз энергетического комплекса представляется несовершенным. Это обусловлено низкой готовностью нормативно-правовой базы к мас-

штабному внедрению цифровых технологий, интеграции их в бизнес-процессы, фактическое отсутствие единых стандартов и систем сертификации.

К проблемам правового регулирования цифровой трансформации в энергетической отрасли можно отнести отсутствие механизмов упрощенной закупки для компаний с государственным участием инновационной продукции, практическое отсутствие российских комплексных пакетов программного обеспечения, являющихся аналогами зарубежных продуктов [2].

Решение обозначенных проблем требует внедрения системных решений, что неизбежно ведет к росту издержек.

Кроме того, основные нормы, опосредующие деятельность в сфере энергетики, лежат в области регулирования публичного права, в то время как необходим частноправовой механизм правового регулирования энергетики в связи с проведением процессов цифровизации. Это позволит минимизировать затраты по обеспечению масштабирования цифровизации энергетического комплекса путем входа на рынок предприятий без государственного участия, а также в перспективе приведет к получению результатов повышения уровня услуг, предоставляемых конечному потребителю. Цифровизация энергетики детерминирует особую обязанность государства по охране интересов граждан вследствие включения их в процесс внедрения и обязательности применения гражданами новых технологических решений (в частности, «умных» приборов учета) [5. С. 13].

На наш взгляд, учитывая традиционность сферы энергетики и вызовы современности, правовые механизмы проведения цифровизации энергетики должны аккумулировать необходимые черты государственно-правового и частноправового регулирования. Так, должна быть разработана и нормативно обеспечена единая система управления, координации и мониторинга цифровой трансформации энергетического комплекса. Это необходимо в целях появления централизованного подхода к цифровому развитию государственных органов.

Видится необходимым снятие законодательных и финансовых ограничений привлечения инвестиций для обеспечения цифровых технологий в энергетике; развитие мер государственной поддержки разработки и внедрения цифровых энергетических решений. Последнее утверждение призвано обеспечить баланс государственно-правовых и частноправовых интересов. Заказчиками технологий могут выступать государственные компании, в то время как разработчиками технологий – компании, принадлежащие к частному сектору экономики.

При этом целесообразно разработать механизм мер государственной поддержки внедрения цифровых решений в энергетическом комплексе. Прозрачные правовые механизмы подобного рода будут призваны снизить бюрократические барьеры, которые в настоящее время являются серьезным препятствием внедрения цифровых решений, адаптированных под нужды топливного комплекса, а следовательно, и достижению целей всей цифровой экономики.

В декабре 2021 г. было издано распоряжение Правительства Российской Федерации № 3924-р «Об утверждении стратегического направления в области цифровой трансформации топливно-энергетического комплекса» [1]. Распоряжение обозначило основные стратегические направления в области цифровой трансфор-

мации энергетики, а также закрепило приоритеты, цели и задачи цифровой трансформации, кроме того, распоряжение содержало указания на проблемы и вызовы в области цифровизации энергетического комплекса. Можно заключить, что на сегодняшний день этот нормативный правовой акт представляется наиболее комплексным документом, аккумулирующим вектор развития цифровизации энергетической отрасли и проблемы, которые необходимо преодолеть в процессе цифровой трансформации. В частности, распоряжение указывает на существующую необходимость создания инструментов, позволяющих снизить затраты потребителей на покупку электрической энергии, улучшения качества обслуживания клиентов-граждан, оптимизацию затрат электроэнергетической отрасли. Таким образом, именно анализируемое распоряжение Правительства РФ учитывает частноправовую составляющую правоотношений в энергетической отрасли.

На наш взгляд, приведенные нормативные правовые акты не могут в настоящее время регулировать даже часть проблем, возникающих в области объективно необходимой цифровизации энергетики. Положения их абстрактны и декларативны. Без адекватной правовой базы нет возможности разработать механизм полноценного внедрения и использования в исследуемой отрасли цифровых технологий, право связывает технологический прогресс, в глобальном смысле не дает развиваться обществу и государству.

Решением видится выработка единого унифицированного подхода, который стал бы результатом работы специалистов в области технологий и юристов. Такой подход должен учитывать не только общие направления цифровизации, а ее конкретные направления, сообразно очередности и поэтапной необходимости. Правоведы должны учесть такие направления с учетом существующих предложений науки и практики, с последующей разработкой единого нормативного правового акта в форме федерального закона. Такой федеральный закон должен стать базисом для последующего правового регулирования цифровизации энергетической отрасли в целях повышения качественного ее потенциала и учета интересов общества, государства, личности.

Список литературы

1. Распоряжение Правительства Российской Федерации от 28.12.2021 № 3924-р «Об утверждении стратегического направления в области цифровой трансформации топливно-энергетического комплекса» // Собрание законодательства РФ. 2022. № 1. Ст. 398.

2. Рекомендации «круглого стола» Комитета Государственной Думы по энергетике на тему «Законодательное обеспечение развития цифровой энергетики в России». Утверждены Решением Комитета Государственной Думы по энергетике № 3.25–5/81 от 18 июля 2018 года // Официальный сайт Комитета Государственной Думы по энергетике. URL: http://komitet2–13.km.duma.gov.ru/Rabota/Rekomendacii-po-itogam-meropriyatij/item/16637855/ (дата обращения: 09.09.2022).

3. Бушуев В. В., Новиков Н. Л., Новиков А. Н. Цифровизация экономики и энергетики: перспективы и проблемы // Экономические стратегии. 2019. Т. 21, № 6 (164). С. 96–105.

4. Пронина Е. В. Цифровизация российских электрических сетей. Проблемы правового регулирования // Вестник НИБ. 2019. № 38. С. 68–72.

5. Хамидуллин М. Т. Цифровизация договорных отношений с потребителями в сфере энергетики // Юрист. 2022. № 4. С. 12–15.

6. Хитрых Д. О цифровой трансформации энергетической отрасли // ЭП. 2021. № 10 (164). С. 78–89.

7. Хурбатова Ю. В. Цифровизация энергетики – новый вектор развития // Инновации. Наука. Образование. 2021. № 39. С. 224–228.

Н. О. Сабанина,
кандидат исторических наук, доцент,
Международный инновационный университет,
Новомосковский институт
С. А. Попов,
кандидат технических наук, доцент,
Международный инновационный университет,
Новомосковский институт

РОЛЬ ПРАВОВЫХ ИДЕЙ МЫСЛИТЕЛЕЙ ДРЕВНЕГО РИМА ДЛЯ ОСМЫСЛЕНИЯ ПРОБЛЕМАТИКИ ПОНЯТИЯ «ВИРТУАЛЬНОЕ ЛИЦО» В СОВРЕМЕННОЙ ПРАВОВОЙ ДЕЙСТВИТЕЛЬНОСТИ

Аннотация. Наследие римской правовой культуры прослеживается практически во всех сферах современной правовой действительности. Возможность рецепции юридических и политических форм, созданных римской цивилизацией, и их частичная инкорпорация в современную правовую и политическую действительность России, конечно с учетом их осмысления, связанного с особенностями современного развития политических и правовых институтов, актуализирует представленную проблематику. Особенно значима рецепция римского права в области цивилистики. В данной статье проведен анализ роли римского правового наследия, которое может послужить основой для изучения проблематики виртуального субъекта права современной правовой наукой.

Ключевые слова: римское право, виртуальное лицо, рецепция, субъект, влияние, мысль, понятие, история

THE ROLE OF THE LEGAL IDEAS OF THE THINKERS OF ANCIENT ROME FOR UNDERSTANDING THE PROBLEMS OF THE CONCEPT OF “VIRTUAL PERSONALITY” IN MODERN LEGAL REALITY

Abstract. The legacy of Roman legal culture can be traced in almost all spheres of modern legal reality. The possibility of reception of legal and political forms created by the Roman civilization and their partial incorporation into the modern legal and political reality of Russia, of course, taking into account their understanding associated with the peculiarities of the modern development of political and legal institutions actualizes the presented problems. The reception of Roman law in the field of civil law is especially

significant. This article analyzes the role of the Roman legal heritage for the study of the problems of the virtual subject of law by modern legal science.

Keywords: Roman law, Legal entity, Reception, Subject, Influence, Thought, Concept, History

Римское право представляет собой правовую систему, ставшую прообразом правовых систем целого ряда стран мира. Наибольшее значение рецепция римского права имеет для стран романо-германской правовой семьи.

Обратимся к дефиниции категории «рецепция». Рецепция – это понятие, которое имеет латинские корни и означает буквально восприятие, заимствование.

По мнению С. В. Ткаченко, рецепция – это, прежде всего, заимствование идей, правовых институтов, норм, терминологии, присущих иностранному государству, с целью их последующего внедрения в собственную правовую систему [8].

Таким образом, рецепция в праве опосредована, прежде всего, возможностью цивилизационной преемственности, носящей правовой характер.

Причин обращения к достижениям иных правовых систем может быть множество, среди них следует выделить модернизационные процессы, происходящие в правовой системе того или иного государства, необходимость приобщения к достижениям цивилизации, историческую преемственность права государства, зарекомендовавшего себя как наиболее устоявшееся и конструктивное и пр.

Бесспорно, римское право легендарно. Его актуальность обусловлена и проверена временем.

Рецепция римского частного права характерна, прежде всего, для европейской цивилизации, создавшей свою государственность на территории бывшей Римской империи [5.С. 76].

В качестве яркого примера можно привести Гражданский кодекс Франции (так называемый Кодекс Наполеона с соответствующими изменениями), который построен по принципу правового документа Древнего Рима и включает в себя три книги: о лицах, об имуществе и о способах приобретения права собственности. Проводя параллели с римским правом, следует обратиться к Институциям Гая, в которых мыслитель отмечал, что все право Рима относится либо к лицам, либо к вещам, либо к искам [7. С. 115].

Примером может служить и Германское гражданское уложение, построенное по строгой научной «пандектной» системе. Его основой стали Дигесты (пандекты) Юстиниана, императора, по приказу которого была проведена кодификация римского частного права.

К вопросу о признании рецепции римского права российской правовой системой в различные исторические промежутки развития нашего государства и общества исследователи относились по-разному.

В частности, советский исследователь И. Б. Новицкий отмечал, что право – это не что иное, как надстройка над базисом, в силу этого никаким «писаным разумом», о котором говорили мыслители Древнего Рима, оно быть не может. Кроме того, Рим – государство рабовладельческое, в силу этого его право не может быть примером для права Советского государства [4].

Подобного рода позиция оставалась господствующей (с определенными нюансами) на протяжении всего периода существования советского государства.

Начиная с 1990 гг. прошлого столетия происходит реципирование основных положений римского права и повышение его авторитета в среде российских исследователей. Связан данный процесс был с демократизацией правовых и политических процессов, которые шли во многом с опорой на европейский опыт. А правовые системы стран Европы во многом базируются на римской правовой мысли.

Однако если обратиться к исторической и духовной составляющей развития России, то наше государство просто не могло не воспринять нормы римского права и правовую мысль римских юристов.

От Византии – восточного обломка Римской империи – Русь получила христианство, как результат – рецепция византийского права, базой которого стал Кодекс Юстиниана.

Кроме того, на Руси в период христианизации распространялась духовно-правовая литература, созданная в Византии. В качестве примера можно привести широкомасштабное использование Кормчей книги, основу которой составляло законодательство Византии.

Помимо этого документа, можно также назвать те, которые имели чисто византийское происхождение и использовались в правовой системе средневековой Руси, в частности:

1. Свод законов, систематизированных патриархом Константинопольским Иоанном Схоластиком в VI в.

2. Эклог императоров Льва III и Константина V.

3. Номоканон патриарха Фотия (IX).

4 Судный закон.

5. Свод законов императоров Романа и Константина (X в.).

6. Свод законов императора Алексея Комнена.

Были и продукты отечественных законодателей, но существенное влияние на их создание также оказало законодательство Древнего Рима. В частности, это:

1. Пространная Русская Правда.

2. Церковные уставы князей Владимира и Ярослава.

3. Судебник 1497 г. [3].

Период реформаторской деятельности Петра I в области права также во многом базировался на теории и практике римского права. В частности, была проведена кодификационная работа, внесены существенные изменения в юридическую технику. Для данного исторического витка характерно возникновение целого ряда инновационных для этого времени направлений правовой кодификационной мысли законодателя, в частности: право на разработку недр, вексельное право и пр. Кроме того, законодательные источники теперь приобрели исключительно формальный характер.

Кроме того, если мы обратимся к рассмотрению дореволюционного гражданского права, то для него была характерна пандектная система, свойственная римскому праву.

Таким образом, к факторам, определявшим роль и место римского права в России дореволюционного периода, следует отнести:

1. Систематизацию законодательства.

2. Возникновение российской юриспруденции.

3. Сложившуюся судебную практику (например, кассационная практика Судебного департамента Правительствующего Сената).

4. Единые с европейскими подходы к преподаванию юридических дисциплин.

5. Научные контакты с европейскими учеными (это и научные школы, и обучение за границей).

Советский период характеризуется, как мы уже отмечали ранее, неоднозначным подходом к восприятию римского права, прежде всего, по идеологическим причинам, в частности, в связи с тем, что древнеримское государство было рабовладельческим.

В частности, несмотря на негативное отношение к римскому праву, в советский период использовались механизмы рецепции римского права в отношении обязательств, посредством развития научно-правовой доктрины, юридического образования, использования основополагающих начал, присущих римскому праву. Однако принципы, разработанные древнеримскими мыслителями, связанные с правами общечеловеческими ценностями, зачастую носили декларативный характер.

Для современного права воздействие наследия правовой и государственной мысли древнеримской цивилизации по-прежнему весьма актуально. В частности, понятийный аппарат, философия права, юридическая практика, частично методика юридического образования во многом восприняли принципы римского права [1].

Если говорить о влиянии римской правовой и политической мысли на политико-правовую действительность современной России, то следует, прежде всего, обратиться к особенностям современного гражданского законодательства, а также к вопросу о возможности правового регулирования виртуального лица как субъекта права с попыткой найти аналогии подобных субъектов в римском праве.

Современное отечественное гражданское законодательство испытывает влияние римского права, примером тому служит целый ряд законодательных положений, регулирующих имущественные и неимущественные отношения, в частности: определение набора прав и обязанностей, присущих субъектам права, нормы, регулирующие исковую давность, отдельные положения, регулирующие право собственности и обязательственные права, наследственные права и пр. [6].

Полагаем, что одним из поистине гениальных предтечей современной правовой мысли стала разработка в римском праве понятия «виртуальное лицо». Данная категория в настоящее время для российской правовой науки является дискуссионной [2]. В Риме же был подобный субъект – под ним понимались боги. Примечательно, что отношения с богами у римлян строились наподобие торговых сделок (ты – мне, я – тебе). Если боги не выполняли просьбу, то они могли ожидать непочтительности со стороны римлян.

Вышеназванные отношения вполне могут проецироваться на рассмотрение современных правоотношений, которые складываются между такими субъектами права, как физические и виртуальные лица [9].

Считаем, что более подробное рассмотрение предложенного римским правом эквивалента виртуального лица поможет современной правовой доктрине

в более глубоком понимании и, как следствие, правовом регулировании современного виртуального лица.

Тем более что новые правоотношения, порожденные телекоммуникационным миром, нуждаются в правовом регулировании и подробной регламентации отдельного правового статуса субъектов виртуальных отношений.

Анализ различных подходов к пониманию «виртуальный субъект» позволил дать следующее определение данной категории. Итак, виртуальный субъект – это субъект, обладающий неустойчивыми признаками и характеристиками, но способный вступать в правоотношения, например, в сети Интернет и, как следствие, данные правоотношения способны повлечь юридически значимые последствия.

Наблюдаются случаи, когда виртуальные субъекты практически полностью повторяют структурные характеристики и особенности, присущие реальным субъектам правоотношений. В качестве примера можно привести негосударственные интернет-структуры, сообщества физических лиц, носящих виртуальный характер, транснациональных интернет-корпораций и др.

Полагаем, что для того, чтобы произошла индивидуализация субъекта виртуальной среды, необходимо применение процедур технологического характера, в частности, установления его доменного имени, IP-адреса и др.

Кроме того, считаем, что законодателю необходимо уделить должное внимание проработке характеристик, присущих виртуальным субъектам в целях их идентификации.

Таким образом, римская цивилизация дала миру множество достижений, в плеяде которых следует выделить право, ставшее основой для формирования правового мышления и правовой культуры европейских государств.

Россия, право которой основывается на романо-германской правовой семье, также не избежала влияния римского правового наследия. В нашем государстве имеет место рецепция не только норм, институтов и конструкций римского права, но и его принципов.

Основополагающие начала римской правовой мысли во многом стали фундаментом для терминологии, правовой доктрины и правоприменительной практики современных нам государств. Правовая культура Древнего Рима стала тем неисчерпаемым источником, который до сих пор питает современную правовую мысль.

Анализ различных подходов к пониманию «виртуальный субъект» позволил дать следующее определение данной категории. Итак, виртуальный субъект – это субъект, обладающий неустойчивыми признаками и характеристиками, но способный вступать в правоотношения, например в сети Интернет, и, как следствие, данные правоотношения способны повлечь юридически значимые последствия.

Список литературы

1. Encyclopedic dictionary of Roman law. Philadelphia, 1991. 476 p.

Т. А. Савельева,
кандидат юридических наук, доцент,
Новосибирский юридический институт (филиал)
Томского государственного университета

ЦИФРОВИЗАЦИЯ: ЗАЩИТА СЛАБОЙ СТОРОНЫ ДОГОВОРА

Аннотация. Автор рассматривает процесс цифровизации как преобразование социально-экономических систем. Анализирует правовые аспекты и проблемы, возникающие в правоприменительной практике при заключении договоров в электронной форме. Электронный документооборот между участниками рынка опосредует имущественные отношения. При использовании электронных средств характер и содержание самого гражданского правоотношения между сторонами не меняется, не возникает при этом и новой формы сделки.

Ключевые слова: электронный документ, электронная подпись, договор, сделка, гражданское право, юридически значимые действия, защита интересов слабой стороны договора, информационная асимметрия

DIGITALIZATION: PROTECTION OF THE WEAK SIDE OF THE CONTRACT

Abstract. The author considers the digitalization process as a transformation of socio-economic systems. Analyzes the legal aspects and the problems that arise in law enforcement practice when concluding contracts in electronic form. Electronic document flow between market participants mediates property relations based on equality. When using electronic means, the nature and content of the civil legal relationship between the parties does not change, nor does a new form of transaction arise.

Keywords: Electronic document, Electronic signature, Contract, Transaction, civil law, Legally significant actions, Protecting the interests of the weak party of contracts, Information asymmetry

Введение. Вопросы защиты интересов слабой стороны договора не теряют своей актуальности на протяжении всего существования правовой регламентации договорных отношений. Особую значимость они приобретают в эпоху цифровизации, которая меняет многие традиционные подходы гражданского права, включая представления о договоре, правоотношении, обязательстве. Очевидно, что оценка эффективности процесса цифровизации различных сфер жизни должна осуществляться через призму соблюдения интересов слабой стороны договора. В противном случае не будут достигнуты цели цифровизации, одной из которых является совершенствование социальной сферы жизни общества.

При заключении и исполнении договора с использованием цифровых технологий под слабой стороной необходимо понимать всякого пользователя информационного ресурса в силу информационной асимметрии между пользователем и обладателем информационного ресурса.

За рамки настоящей работы выходит анализ смарт-контрактов, заключаемых и исполняемых зачастую без участия человека. По поводу их правовой природы,

возможности применения к ним традиционных конструкций договорного и обязательственного права высказаны разные точки зрения, что свидетельствует об активном поиске юридическим сообществом ответов на многие животрепещущие вопросы [1. С. 35–41; 15. С. 32–60]. Представляется, что одним из таких вопросов, который потребует взвешенного ответа, является вопрос о статусе субъектов возникающего правоотношения, распределения рисков между ними. В настоящей же статье автор сосредоточился, возможно, на более приземленных, но не менее актуальных вопросах защиты интересов слабой стороны в более простых договорных конструкциях, по сравнению со смарт-контрактом.

Основная часть. Говоря о процессе цифровизации, следует исходить из того, что он носит глобальный характер, затрагивает все сферы деятельности человека. В литературе справедливо отмечено, что цифровизация является коренным преобразованием функционирования социально-экономических систем всех уровней [3. С. 6].

Правовая сфера не является исключением. Напротив, процесс цифровизации немыслим вне права, поскольку нуждается в правовой регламентации. При этом само право, являясь одной из социальных систем, испытывает на себе влияние процесса цифровизации.

В качестве примера можно привести положения Концепции развития технологий машиночитаемого права, утвержденной в 2021 г. Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности [6].

Под машиночитаемым правом понимается «основанное на онтологии права изложение определенного набора правовых норм на формальном языке (в том числе языке программирования, языке разметки), а также технологии машиночитаемого права (инструменты применения таких норм в виде необходимых информационных систем и программного обеспечения)». Авторы концепции отмечают, что на текущем уровне развития технологий машиночитаемого права машиночитаемые нормы дополняют, а не заменяют собой нормы, написанные на естественном языке. В дальнейшем предполагается, что «развитие машиночитаемого права, возможно, приведет к его преобладанию в законодательном массиве над нормами, изложенными на естественном языке. В свою очередь нормы на естественном языке будут представлять собой производное изложение норм формального языка на естественном языке» [6. С. 2–4].

В практической плоскости цифровые технологии уже сегодня облегчают обмен информацией, совершение сделок и их исполнение. Все это делает нашу жизнь более удобной и комфортной, оформление документов оперативным, получение услуг более доступным.

Говоря о гражданско-правовой сфере, следует отметить достаточно широкое распространение заключения соглашений через интернет-сайты, посредством электронного документооборота, развитие системы смарт-контрактов и т. п.

Развитие цифровых технологий, безусловно, влечет трансформацию порядка заключения договоров, их исполнения. Однако при такой трансформации возни-

кают риски как для участников гражданского оборота, так и правопорядка в целом. Эти риски нуждаются в осмыслении и выработке мер по их минимизации. Представляется, что во главе угла должен стоять вопрос защиты интересов слабой стороны.

Через призму соблюдения баланса интересов сторон рассмотрим вопросы заключения договоров в электронной форме.

В силу п. 1 ст. 160 Гражданского кодекса Российской Федерации (далее – ГК РФ, Кодекс) [2] сделка в письменной форме должна быть совершена путем составления документа, выражающего ее содержание и подписанного лицом или лицами, совершающими сделку, либо должным образом уполномоченными ими лицами. Письменная форма сделки считается соблюденной также в случае совершения лицом сделки с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки, при этом требование о наличии подписи считается выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. Законом, иными правовыми актами и соглашением сторон может быть предусмотрен специальный способ достоверного определения лица, выразившего волю.

С 01.10.2019 законом предусмотрена возможность заключить в электронном виде договор, к которому предъявляется требование его заключения путем составления одного документа [7].

Напомним, что требование о заключении договора путем подписания одного документа распространяется на большинство сделок с недвижимым имуществом (ст. 550, 560, 651, 658 ГК РФ). Путем подписания одного документа подлежит заключению также корпоративный договор (ст. 67.2 ГК РФ), договор о создании акционерного общества (ст. 98 ГК РФ) и др.

В п. 2 ст. 434 ГК РФ в новой редакции закреплено, что договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграммами, электронными документами либо иными данными в соответствии с правилами абзаца 2 п. 1 ст. 160 Кодекса.

Рассмотрим в рамках рассматриваемой проблематики защиты интересов слабой стороны порядок заключение договора через интернет-сайты.

Общее правило состоит в том, что договор заключается путем согласия пользователя с размещенной на сайте офертой, содержащей условия договора (соглашения). Предполагается, что до выражения согласия пользователь предварительно ознакомился с условиями договора. Ознакомление с условиями договора (офертой, размещенной на сайте) и выражение воли заключить договор (акцент) возможны в нескольких вариациях.

Оферта (под названием «договор», «соглашение», «условия» и т. п.) может быть размещена непосредственно на сайте. Пользователь, нажимая кнопку, подтверждает свое согласие с офертой, всеми ее условиями. В данном случае тот факт, что пользователь, нажимая кнопку, не ознакомился с условиями будущего договора, мало чем отличается от последствий подписания договора в бумажном виде, усло-

вия которого не были прочитаны стороной. Говорить здесь о нарушении интересов слабой стороны, которая не прочитала условия договора, является излишним.

Другим вариантом, который используется на практике, является предоставление пользователю возможности ознакомиться с условиями договора путем перехода по гиперссылке. При этом информационная система позволяет нажать кнопку о согласии с условиями договора в случае, если пользователь не перешел по гиперссылке и не ознакомился с условиями договора. В этом случае правовые последствия наступают такие же, как если бы он ознакомился с условиями договора. Договор считается заключенным.

Проводя параллель с заключением договора в традиционной письменной форме можно в качестве аналога привести подписание сторонами договора, содержащего ссылку на некий иной документ. Примером может служить заключение договора потребительского кредита (займа). В силу статьи 5 Закона «О потребительском кредите (займе)» договор потребительского кредита (займа) состоит из общих условий и индивидуальных условий [9]. Если заемщик подписал индивидуальные условия, не изучив общие условия, то договор потребительского кредита (займа) считается заключенным. Аналогичная ситуация возникает при заключении договора банковского счета, содержащего ссылки на тарифы и т. д.

Представляется, что интересы пользователя могут быть нарушены, но не в силу специфики электронной формы договора, а в силу неравенства переговорных возможностей, характерных и для заключения договора в традиционной письменной форме. Об этом будет сказано далее.

Еще одним распространенным вариантом выражения пользователем своего согласия на заключение договора является, по сути, бездействие пользователя в ситуации, когда на сайте высвечивается надпись о том, что, продолжая пользоваться сайтом, пользователь выражает согласие с условиями соглашения. Особенность в данном случае состоит в том, что пользователь не выражает явно своей воли, своего согласия с условиями.

В данном случае требует осмысления вопрос о том, следует ли признавать договор заключенным. Возможные аргументы о том, что пользователя можно считать выразившим волю на заключение договора в силу п. 3 ст. 438 ГК РФ являются сомнительными, поскольку указанная норма рассматривает в качестве акцепта действия по выполнению указанных в оферте условий договора. В рассматриваемой нами ситуации речь идет не о совершении действий, а о бездействии со стороны пользователя. Расширительное толкование нормы, предусмотренной п. 3 ст. 438 ГК РФ, может служить почвой для нарушения интересов слабой стороны.

Очевидно, что универсальный ответ дать невозможно, поскольку конкретные обстоятельства относительно способа визуализации условий договора на сайте могут существенным образом различаться [4. С. 49–57].

Представляется, что возложение на пользователя каких-либо обязанностей, вытекающих из условий соглашения, прямого согласия с которыми он явно не выражал, нарушает баланс интересов сторон.

Даже в случае, если мы признаем соглашение заключенным, требования к пользователю, основанные на условиях соглашения, необходимо оценивать ис-

ходя из того, что пользователь должен признаваться слабой стороной в силу информационной асимметрии. Поведение владельца сайта должно оцениваться через призму соблюдения им принципа добросовестности (ст. 1, 10 ГК РФ).

В целях правовой определенности целесообразно на законодательном уровне ввести ограничения на использование указанного способа заключения договора и предусмотреть способы защиты слабой стороны.

В целом говоря о заключении договора посредством интернет-сайтов, необходимо исходить из того, что пользователь во всех случаях должен признаваться слабой стороной, исходя из неравенства переговорных возможностей. Представляется, что все соглашения, заключенные посредством интернет-сайтов, относятся к договорам присоединения (ст. 428 ГК РФ).

В соответствии с п. 1 ст. 428 ГК договором присоединения признается договор, условия которого определены одной из сторон в формулярах или иных стандартных формах и могли быть приняты другой стороной не иначе как путем присоединения к предложенному договору в целом.

Присоединившаяся сторона является слабой в силу неравенства переговорных возможностей и имеет, как известно, гарантии, в случае если договор содержит обременительные условия. Присоединившаяся сторона наделяется правом требовать изменения или расторжения договора с ретроспективным эффектом (п. 2 ст. 428 ГК РФ).

Заслуживает безусловной поддержки введение в ходе реформы гражданского права нормы, указанной в п. 3 ст. 428 ГК РФ. С этого момента гарантии в виде расторжения или изменения договора распространяются на случаи, если при заключении договора, не являющегося договором присоединения, условия договора определены одной из сторон, а другая сторона в силу явного неравенства переговорных возможностей поставлена в положение, существенно затрудняющее согласование иного содержания отдельных условий договора.

Представляется, что во всех договорах, заключаемых через интернет-сайты, соответствуют критериям, предусмотренным ст. 428 ГК РФ, а именно:

1) определение условий соглашения только одной из сторон;

2) неравенство переговорных возможностей.

Неравенство переговорных возможностей обусловлено тем, что владелец сайта профессионально владеет информацией. Что касается второго критерия, то он также имеется, так как условия договора определяются только одной стороной, а другая сторона только принимает эти условия и не может влиять на их содержание.

В литературе применительно к договорам страховых услуг, заключаемых в электронной форме, высказано мнение о том, что «механизмы защиты, которые заложены в п. 3 ст. 428 ГК РФ, не могут быть реализованы в полной мере. Речь идет об отсутствии в законодательстве определенных критериев, позволяющих на практике «расшифровать» (или конкретизировать), имеются ли в правоотношениях неравенство переговорных возможностей и определение условий договора только одной из сторон, которые дают слабой стороне названные правовые гарантии» [12. С. 73–81].

Обозначенная проблематика действительно имеется. Однако применительно к договорам, заключаемым посредством интернет-сайтов, закрепление законодательных критериев является излишним. Толкование ст. 428 ГК позволяет сделать вывод, что все соглашения, заключаемые посредством интернет-сайтов, должны подпадать под сферу регулирования ст. 428 ГК РФ. Соответственно, слабая сторона наделяется гарантиями в виде возможности расторжения или изменения договора при наличии обременительных условий с ретроспективным эффектом. В целях единообразия судебной практики было бы целесообразным, чтобы Верховный суд РФ закрепил подобное толкование статьи 428 ГК РФ применительно к сделкам, заключаемым через интернет-сайты, в виде соответствующего разъяснения.

Такой подход для продавцов или исполнителей, реализующих свои товары, услуги через интернет-сайты, является достаточно строгим, поскольку ограничивает их возможности по включению в текст оферты, размещаемой на сайте, ряда выгодных условий в силу риска их оспаривания в рамках статьи 428 ГК РФ. В данном случае действует правило о том, что чем жестче в свою пользу контрагент формулирует условия договора, тем менее устойчивыми они являются.

В будущем для снятия данных рисков следует ожидать, что на сайтах появятся опции, предоставляющие пользователю возможность предлагать альтернативные условия соглашения, с тем чтобы вывести данные соглашения из сферы действия ст. 428 ГК РФ.

Таким образом, изложенное позволяет прийти к выводу, что при заключении договоров через интернет-сайты пользователь является слабой стороной в силу информационной асимметрии, неравенства переговорных возможностей. К отношениям сторон должны применяться правила ст. 428 ГК РФ, наделяющие слабую сторону правом изменения или расторжения договора, содержащего обременительные условия, с ретроспективным эффектом.

Далее рассмотрим некоторые аспекты заключения договора в электронной форме путем подписания одного документа. В этом случае обе стороны подписывают документ своими электронными подписями.

Как известно, отношения в области использования электронных подписей при совершении гражданско-правовых сделок регулируются специальным законом «Об электронной подписи» [11].

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (ст. 2 Закона об электронной подписи).

Закон об электронной подписи выделяет простую и усиленную электронную подпись, последняя делится на квалифицированную и неквалифицированную электронную подпись (ст. 5 Закона).

Наибольшей юридической силой обладает квалифицированная подпись в силу того, что информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью,

и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации (п. 1 ст. 6 Закона об электронной подписи).

Здесь хотелось бы обратить внимание, что применительно к недвижимости допускается не только заключение договора, но и подписание документа о передаче недвижимости в электронной форме.

Представляется, что оформление приема-передачи имущества в электронной форме, столь удобное и используемое на практике, таит в себе риски, непредсказуемые для сторон.

Отметим, что законодателем в сфере отношений по купле-продаже установлен механизм, обеспечивающий баланс интересов сторон при обнаружении недостатков в проданном товаре. По договору продажи недвижимости законодателем установлен специальный порядок передачи предмета купли-продажи продавцом покупателю. В силу ст. 556 ГК РФ передача недвижимости продавцом и принятие ее покупателем осуществляются по подписываемому сторонами передаточному акту или иному документу о передаче. Если иное не предусмотрено законом или договором, обязательство продавца передать недвижимость покупателю считается исполненным после вручения этого имущества покупателю и подписания сторонами соответствующего документа о передаче.

Установленный законодателем специальный порядок исполнения продавцом обязанности по передаче имущества обусловлен рядом причин. Акт приема-передачи, подписанный сторонами, является доказательством передачи недвижимости по договору купли-продажи. Подписание акта влечет переход владения на недвижимую вещь от продавца к покупателю. Покупатель становится законным владельцем объекта недвижимости и имеет право на защиту своего владения на основании ст. 305 ГК РФ (см. п. 60 Постановления Пленума Верховного Суда Российской Федерации № 10, Постановления Пленума Высшего Арбитражного Суда Российской Федерации № 22 от 29.04.2010) [8].

Кроме того, акт приема-передачи, как правило, содержит описание состояния недвижимости и может служить доказательством относительно качества передаваемого объекта недвижимости, его соответствия условиям договора купли-продажи.

На практике встречаются случаи, когда стороны используют электронную форму подписания не только договора купли-продажи, но и в электронной форме фиксируют факт приема-передачи имущества. Такая потребность зачастую возникает в ситуации, когда покупатель заинтересован в приобретении недвижимости вне места своего проживания или нахождения.

Представляется, что уровень рисков для участников сделки является незначительным, если взаимоотношения сторон построены таким образом, что покупатель заранее знакомится с объектом недвижимости лично или через представителя, а процесс достижения консенсуса с продавцом осуществляется дистанционно с оформлением самой сделки и акта приема-передачи в электронной форме в относительно короткий период времени с момента личного ознакомления покупателя с объектом недвижимости. В этом случае возникает единственный вопрос – о процедуре передачи ключей продавцом покупателю, которые находятся в разных населенных пунктах.

Если же процесс согласования условий затягивается во времени, а последующее подписание покупателем договора продажи недвижимости, и особенно акта приема-передачи недвижимости осуществляется дистанционно в электронной форме, без дополнительного ознакомления покупателем с состоянием объекта недвижимости, то следует констатировать возникновение рисков у покупателя. Ведь он подписывает акт приема-передачи без ознакомления с текущим состоянием объекта недвижимости, что может создать в будущем значительные трудности в процессе доказывания недостатков переданного объекта недвижимости.

Уровень рисков еще более возрастает в ситуации, когда покупатель без предварительного личного ознакомления с состоянием объекта дистанционно совершает сделку с одновременным оформлением приема-передачи имущества. В таких случаях покупатель дистанционно общается с продавцом, а относительно состояния недвижимости полагается на представленную продавцом информацию, включая показ недвижимости по видео и т. п.

Следует отметить, что риски возникают у обеих сторон. Покупатель может столкнуться с тем, что состояние недвижимости не соответствует тому, как оно было показано продавцом дистанционно путем видеосвязи. Процесс доказывания для покупателя будет осложнен, поскольку результаты показа не зафиксированы. Кроме того, покупатель в данном случае, подписав акт приема-передачи, фактически не получает владение недвижимостью.

Для продавца такое оформление сделки и акта приема-передачи также может создать проблемы. Так, недобросовестный покупатель получает возможность ставить вопрос о том, что он заключил сделку под влиянием обмана или заблуждения, поскольку не осматривал объект недвижимости. Кроме того, покупатель может также ставить вопрос о том, что фактической передачи недвижимости не было, подписание акта носило фиктивный характер. Ссылаясь на указанные обстоятельства, покупатель может ставить вопрос о признании факта приема-передачи недвижимости несостоявшимся, а самого акта мнимым (по аналогии п. 1 ст. 170 ГК РФ). Не смотря на подписание акта, покупатель может ставить вопрос об ответственности продавца за нарушение обязанности по передаче имущества.

Таким образом, приведенные примеры наглядно иллюстрируют, что использование электронной формы для фиксации передачи объекта недвижимости по договору продажи в сочетании с подписанием договора в электронной форме влечет риски для участников гражданского оборота, что требует регламентации ряда важных вопросов, направленных на защиту интересов сторон договора продажи недвижимости.

В частности, актуальным является вопрос о том, когда считается переданным недвижимое имущество при подписании акта приема-передачи в электронной форме. Кто несет риски случайной гибели и повреждения объекта недвижимости при наличии подписанного акта приема-передачи в электронной форме в ситуации, когда материалами дела подтверждено отсутствие фактической передачи владения покупателю? Возможно ли привлечение к ответственности продавца за просрочку передачи имущества при наличии подписанного акта?

Далее, при анализе процесса заключения договора и динамики договорного обязательства с использованием информационных технологий нельзя обойти стороной вопросы обмена электронными сообщениями.

Если обмен электронными сообщениями осуществляется участниками гражданского оборота в рамках ранее заключенного между ними соглашения об осуществлении электронного документооборота, то правовые последствия определяются условиями данного соглашения. **Заключение** подобных соглашений является распространенной практикой, в частности, в сфере банковского обслуживания.

Однако на практике, к сожалению, наиболее распространены случаи ведения переписки по электронной почте в договорной сфере без заключения специальных соглашений по этому поводу, обмен по электронной почте скан-копиями документов и т. п. Это является почвой для споров между участниками гражданского оборота. Следует признать, что судебной практикой не выработано единообразного подхода относительно оценки правовых последствий направления по электронной почте документов, не подписанных электронной подписью.

Здесь, видимо, необходимо разграничить стадии заключения договора и последующего взаимодействия сторон (изменение условий договора, исполнение обязательств).

Что касается стадии заключения договора, то сообщения, направленные по электронной почте и не подписанные электронной подписью, не должны рассматриваться в качестве оферты или акцепта, если сторонами предварительно не было заключено соглашение об электронном документообороте с указанием конкретных электронных адресов, сообщения с которых стороны признают легитимными и подтверждающими выражение воли стороны по сделке.

В соответствии с п. 2 ст. 434, абз. 2 п. 1 ст. 160 ГК РФ договор может быть заключен путем обмена письмами, электронными документами либо иными данными, передаваемыми с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки, при этом требование о наличии подписи считается выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю.

Сравнивая заключение договора в традиционной письменной форме и заключение договора в электронной форме, Л. Г. Ефимова указывает, что «отсутствие требования об обязательном применении подписи при заключении сделок в электронной форме является наиболее серьезным отличием традиционной письменной формы сделки от сделки, заключенной с использованием с помощью электронных либо иных технических средств» [5. С. 129–137].

Предложение о заключении договора (оферта) и ответ на него (полный и безоговорочный акцепт или протокол разногласий) не должны считаться подписанными, если использован способ, не позволяющий определить выразившее волю лицо. Отправление сообщения с адреса электронной почты само по себе (при отсутствии иных подтверждающих обстоятельств) не является способом, позволяющим определить лицо, выявившее свою волю на вступление в договорные отношения.

Иной подход нарушает разумный баланс интересов сторон. Ведь было бы чрезмерным возлагать на лицо, которое всего лишь ведет переписку по электронной почте на преддоговорной стадии, риски того, что с его адреса будет отправлено, возможно по случайности, не санкционированное им сообщение. Отправитель не подтверждал свою идентификацию данным адресом электронной почты.

Иначе должны оцениваться ситуации по взаимодействию сторон в рамках уже заключенного договора, в котором стороны указали свои электронные адреса. Указание адресов в договоре должно расцениваться как подтверждение того, что сообщения, отправляемые с этого адреса, являются выражением воли стороны договора.

Верховный Суд РФ в Постановлении Пленума № 25 от 23.06.2015 дал следующее разъяснение: «Если иное не установлено законом или договором и не следует из обычая либо практики взаимоотношения сторон, юридически значимое сообщение может быть направлено в том числе с помощью электронной почты, факсимильной и другой связи, осуществлено в иной форме, соответствующей характеру сообщения и отношений, информация о которых содержится в нем, и позволяющей достоверно установить, от кого исходило сообщение и кому оно адресовано» (п. 65 Постановления) [10].

Как указал Верховный Суд РФ в п. 66 Постановления, «в юридически значимом сообщении может содержаться информация о сделке (например, односторонний отказ от исполнения обязательства) и иная информация, имеющая правовое значение (например, уведомление должника о переходе права (ст. 385 ГК РФ) [10].

Анализ судебной практики показывает, что суды, применяя нормы права, касающиеся использования электронной формы сделок, не всегда должным образом обосновывают свои выводы при разрешении споров.

В качестве примера можно привести одно из арбитражных дел, в рамках которого рассматривался спор о том, можно ли признать договор заключенным в ситуации, когда одна из сторон ссылалась на то, что при заключении договора возникли разногласия и протокол разногласий не был подписан.

По данному делу суд пришел к выводу о том, что договор заключен. В качестве обоснования суд указал, что в материалы дела представлена копия протокола разногласий, подписанного уполномоченным лицом и направленного другой стороне посредством электронной почты.

Суд сослался на положения п. 19.3 договора, согласно которому все изменения и дополнения к договору могут быть заключены сторонами путем обмена скан-копиями документов, подписанных уполномоченными лицами, с помощью электронной почты, а также на положения п. 2 ст. 434 ГК РФ, в силу которого договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграммами, электронными документами либо иными данными в соответствии с правилами абзаца 2 п. 1 ст. 160 настоящего Кодекса [14].

Вряд ли можно признать аргументацию, приведенную судом, убедительной. Странной выглядит ссылка суда на условия договора в принципе, ведь сам факт заключения договора оспаривается в суде. Кроме того, п. 19.3 договора относился к обмену информацией по вопросам, касающимся дополнения или изменения

договора, и вступил бы в силу только в случае, если бы договор был заключен. Другое дело, что из обстоятельств следует (насколько можно судить из содержания судебного акта), что оплата по договору была произведена. Факт оплаты в совокупности с тем, что наличие проекта договора не оспаривалось стороной, которая его подписала, с протоколом разногласий, позволял квалифицировать действия оспаривающей стороны в качестве акцепта по правилам п. 3 ст. 438 ГК РФ.

Что касается юридически значимых сообщений, направляемых по электронной почте, то интерес представляет подход суда по оценке переписки сторон в электронной форме по одному из дел. Суд не стал оценивать электронную переписку, рассматривать ее как доказательство волеизъявления одной из сторон, мотивируя фактом отсутствия в договоре сторон соглашения о допустимости переписки между сторонами в электронной форме [13].

Представляется, что такой подход суда к переписке сторон является излишне жестким. Если речь идет не о стадии заключения договора, а о направлении юридически значимых сообщений в рамках заключенного договора, то отправка по адресу электронной почты, указанной даже в реквизитах сторон, должна признаваться исходящей от стороны по договору.

Таким образом, изложенное выше позволяет сделать вывод, что использование электронных ресурсов при заключении договора, при его исполнении не меняет существа договора и возникающего на его основе обязательства, которые должны рассматриваться через призму традиционных понятий гражданского права. Следует согласиться с высказанным в литературе мнением о том, что характер и содержание гражданского правоотношения не меняется [16. С. 26–35]. Защита интересов слабой стороны договора требует особого внимания с учетом специфики построения договорных отношений с использованием информационных технологий.

Заключение.

1. Вопросы защиты интересов слабой стороны договора приобретают особую значимость в эпоху цифровизации, которая меняет многие традиционные подходы гражданского права, включая представления о договоре, правоотношении, обязательстве.

2. Оценка эффективности процесса цифровизации различных сфер жизни должна осуществляться через призму соблюдения интересов слабой стороны договора. В противном случае не будут достигнуты цели цифровизации, одной из которых является совершенствование социальной сферы жизни общества.

3. При заключении договоров через интернет-сайты пользователь является слабой стороной в силу информационной асимметрии, неравенства переговорных возможностей. К отношениям сторон должны применяться правила ст. 428 ГК РФ, наделяющие слабую сторону правом изменения или расторжения договора, содержащего обременительные условия, с ретроспективным эффектом.

В будущем следует ожидать, что на сайтах появятся опции, предоставляющие пользователю предлагать альтернативные условия соглашения, с тем чтобы вывести данные соглашения из сферы действия ст. 428 ГК РФ.

4. Законодательство допускает возможность не только заключения в электронной форме договора продажи недвижимости, но и подписание документа о передаче недвижимости продавцом покупателю.

Использование электронной формы для фиксации передачи объекта недвижимости по договору продажи в сочетании с подписанием договора в электронной форме влечет риски для участников гражданского оборота, что требует регламентации ряда важных вопросов, направленных на защиту интересов сторон договора продажи недвижимости.

5. Если обмен электронными сообщениями осуществляется участниками гражданского оборота в рамках ранее заключенного между ними соглашения об осуществлении электронного документооборота, то правовые последствия определяются условиями данного соглашения.

На практике не распространены случаи ведения переписки по электронной почте в договорной сфере без заключения специальных соглашений. Это является почвой для споров между участниками гражданского оборота.

Сообщения, направленные по электронной почте и не подписанные электронной подписью, не должны рассматриваться в качестве оферты или акцепта, если сторонами предварительно не было заключено соглашение об электронном документообороте с указанием конкретных электронных адресов, сообщения с которых стороны признают легитимными и подтверждающими выражение воли стороны по сделке.

Иначе должны оцениваться ситуации по взаимодействию сторон в рамках уже заключенного договора, в котором стороны указали свои электронные адреса. Указание адресов расценивается как подтверждение того, что сообщения, отправляемые с этого адреса, будут являться выражением воли стороны договора.

6. Использование электронных ресурсов при заключении договора, при его исполнении не меняет существа договора и возникающего на его основе обязательства, которые должны рассматриваться через призму традиционных понятий гражданского права. Регламентация внедрения цифровых технологий в сферу договорного регулирования должна включать в себя выработку мер по защите слабой стороны, каковой является, по общему правилу, пользователь информационных ресурсов.

Список литературы

1. Белов В. А. Смарт-контракт: понятие, правовое регулирование, правоприменительная практика, потребительские отношения // Право и экономика. 2021. № 9. С. 35–41.

2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (с изменениями) // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 15.09.2022).

3. Грибанов Ю. И. Цифровая трансформация социально-экономических систем на основе развития института сервисной интеграции: дис. … д-ра экон. наук. Санкт-Петербург, 2019.

4. Гринь О. С. Трансформации требований к форме договоров с учетом развития цифровых технологий // Актуальные проблемы российского права. 2019. № 6. С. 49–57.

5. Ефимова Л. Г. Еще раз о понятии и правовой природе электронной формы сделки // Lex russica. 2019. № 8. С. 129–137.

6. Концепция развития технологий машиночитаемого права: утверждена Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 15.09.2021 № 31 // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 15.09.2022).

7. О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: Федеральный закон от 18.03.2019 № 34-ФЗ // Собрание законодательства РФ.2019. № 12. Ст. 1224.

8. О некоторых вопросах, возникающих в судебной практике при разрешении споров, связанных с защитой права собственности и других вещных прав: Постановление Пленума Верховного Суда РФ № 10, Постановления Пленума Высшего Арбитражного суда РФ № 22 от 29.04.2010 // СПС «Консультант». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 15.09.2022).

9. О потребительском кредите (займе): Федеральный закон от 21.12.2013 № 353-ФЗ (с изменениями и дополнениями) // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 15.09.2022).

10. О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации: Постановление Пленума Верховного Суда РФ от 23.06.2015 № 25 // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 05.09.2022).

11. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ (с изменениями и дополнениями) // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 05.09.2022).

12. Овчинникова Ю. С. Цифровизация страховых услуг: защита слабой стороны договора и частной жизни // Имущественные отношения в Российской Федерации. 2022. № 3. С. 73–81.

13. Постановление Арбитражного суда Центрального округа от 07.06.2020 № Ф10–2378/2020 по делу № А84–3639/2019 // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 05.01.2021).

14. Постановление Четырнадцатого арбитражного апелляционного суда от 23.12.2019 № 14АП-10545/2019 по делу № А13–15256/2019 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 05.09.2022).

15. Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.

16. Шелепина Е. А. Тенденции правового регулирования электронного документооборота в национальном гражданском праве // Право и цифровая экономика. 2021. № 1. С. 26–35.

В. П. Скобелев,
кандидат юридических наук, доцент,
Белорусский государственный университет

О РЕГУЛИРОВАНИИ ВОПРОСОВ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРОЕКТЕ КОДЕКСА ГРАЖДАНСКОГО СУДОПРОИЗВОДСТВА

Аннотация. В статье анализируется, как в проекте Кодекса гражданского судопроизводства урегулированы некоторые вопросы использования современных цифровых технологий. В частности, автор рассматривает правила использования электронных документов для коммуникаций суда и участников судопроизводства, порядок фиксирования хода процесса, процедуру проведения судебных заседаний в дистанционном формате с помощью видео-конференц-связи и иных технических средств. По результатам исследования сделаны рекомендации по совершенствованию норм Кодекса гражданского судопроизводства.

Ключевые слова: гражданское судопроизводство, цифровые технологии, электронный документ, звукозапись, видеозапись, видео-конференц-связь, иные технические средства

ABOUT REGULATION OF QUESTIONS OF USE OF MODERN DIGITAL TECHNOLOGIES IN THE PROJECT OF THE CODE OF CIVIL PROCEDURE

Abstract. The article analyzes how some issues of the use of modern digital technologies are regulated in the draft Code of Civil Procedure. In particular, the author examines the rules for the use of electronic documents for communications between the court and participants in legal proceedings, the procedure for recording the progress of the process, the procedure for holding court sessions remotely using video conferencing and other technical means. Based on the results of the study, recommendations were made to improve the norms of the Code of Civil Procedure.

Keywords: Civil litigation, Digital technologies, Electronic document, Sound recording, Video recording, Videoconferencing, Other technical means

Введение. В Республике Беларусь одним из векторов развития процессуального законодательства был избран путь унификации Гражданского процессуального кодекса Республики Беларусь (далее – ГПК) и Хозяйственного процессуального кодекса Республики Беларусь (далее – ХПК) посредством их замены единым Кодексом гражданского судопроизводства (далее – КГС). К настоящему времени проект КГС уже подготовлен [1] и прошел процедуру общественного обсуждения [2]. В связи с этим интересно обратить внимание на то, каким образом в проекте КГС урегулированы некоторые вопросы использования современных цифровых технологий.

Основная часть. В ч. 4 ст. 5 КГС в качестве общего правила закреплена возможность подачи искового заявления, заявления, жалобы и иных документов в суд «в виде электронного документа в порядке, установленном законодательными

актами». Данная возможность подкреплена более конкретными предписаниями применительно к случаям обращения в суды в определенных видах судопроизводства (в исковом судопроизводстве, в том числе в производстве по коллективному исковому заявлению, – ч. 1 ст. 238, ч. 5 ст. 325 КГС; в приказном производстве – ч. 1 ст. 343, ч. 4 ст. 348 КГС; в производстве об отмене решения третейского суда, международного арбитражного (третейского) суда, иного постоянного арбитражного органа, находящихся на территории Республики Беларусь, – ч. 1 ст. 468 КГС; в производстве о выдаче исполнительного листа на принудительное исполнение решения третейского суда, международного арбитражного (третейского) суда, иного постоянного арбитражного органа, находящихся на территории Республики Беларусь, – ч. 1 ст. 493 КГС; в производстве по заявлению о выдаче исполнительного листа на принудительное исполнение медиативного соглашения – ч. 1 ст. 499 КГС; в производстве о признании и приведении в исполнение решений иностранных судов, иностранных третейских судов (арбитражей) – ч. 1 ст. 530 КГС; в производстве о признании и приведении в исполнение международного медиативного соглашения – ч. 1 ст. 538 КГС) и на проверочных стадиях процесса (в апелляционном производстве – ч. 1 ст. 561 КГС; в кассационном производстве – ч. 1 ст. 594 КГС; надзорном производстве – ч. 1 ст. 617; в производстве о пересмотре судебных постановлений по вновь открывшимся обстоятельствам – ч. 1 ст. 633 КГС).

Однако в ряде случаев КГС предусматривает только письменную форму обращения в суд – по вопросам восстановления утраченного судебного производства (ч. 1 ст. 458) и оспаривания решения трудового арбитража (ч. 1 ст. 475), что, вероятно, можно объяснить некритическим заимствованием соответствующих норм из ГПК, которые допускают возможность подачи документов в суд только в традиционной письменной форме.

По-видимому, под электронным документом в приведенных выше нормах КГС понимается документ в электронном виде, заверенный электронной цифровой подписью. Однако далеко не всегда в тех статьях, которые упоминают о подаче в суд электронного документа, говорится также об электронной цифровой подписи. Указания на электронную цифровую подпись присутствуют только в ч. 6 ст. 238, ч. 4 ст. 343, ч. 4 ст. 468, ч. 4 ст. 493, ч. 5 ст. 530, ч. 5 ст. 538 КГС. Кроме того, ч. 3 ст. 57 КГС содержит довольно абстрактную норму о том, что участвующие в деле лица «вправе представлять в суд документы в электронном виде в установленном законодательством порядке», т. е. вид электронной формы документов не конкретизирован.

Представление документов в электронной форме возможно и в обратном направлении: от суда к участвующим в деле и иным лицам. Так, ч. 3 ст. 57 КГС предусматривает для лиц, участвующих в деле, возможность «получать с использованием глобальной компьютерной сети Интернет копии судебных постановлений, выполненных в форме электронных документов».

В установленном законодательными актами порядке возможно направление судом исполнительного листа для исполнения в форме электронного документа, подписанного судьей электронной цифровой подписью (ч. 4 ст. 480 КГС), а также выдача исполнительного листа взыскателю в форме электронного документа (ч. 7

ст. 480 КГС, в этом случае о необходимости заверения его электронной цифровой подписью норма ничего не говорит).

КГС (ст. 104–107) в целом сохранил правила ГПК (ст. 113, 174–176) и ХПК (ст. 189–189-3) о порядке фиксирования хода процесса, а именно: ход каждого судебного заседания суда первой инстанции, а также ход совершения каждого отдельного процессуального действия суда первой инстанции вне заседания подлежат фиксированию с использованием средств звуко- или видеозаписи и составлением краткого протокола в письменной форме; в случае неявки в судебное заседание всех участников гражданского судопроизводства, а также при отсутствии технической возможности вести звуко- или видеозапись ход судебного заседания или совершения отдельного процессуального действия суда вне заседания фиксируется составлением протокола в письменной форме.

В регламентации фиксирования хода процесса появилась только одна новая, причем, на наш взгляд, некорректная во многих отношениях норма: «В случае принятия судом первой инстанции апелляционной жалобы и (или) апелляционного протеста по делу составляется протокол в письменной форме в соответствии с требованиями, установленными пп. 2–9 ч. 2 ст. 105 настоящего Кодекса» (ч. 6 ст. 106 КГС).

Во-первых, норма получила неверное структурное месторасположение. Ведь норма является не общей (т. е. касающейся всех стадий процесса и видов производства), а специальной (имеющей отношение только к одной стадии процесса и даже более того – лишь к одному из этапов данной стадии). Потому ей следует находиться в гл. 54 КГС «Производство в суде апелляционной инстанции» в § 2 «Возбуждение апелляционного производства».

Во-вторых, норма не соответствует предусмотренным КГС условиям для фиксирования хода процесса посредством составления протокола. Из ч. 3 ст. 104 КГС видно, что ход процесса в суде первой инстанции (а принятием апелляционной жалобы или протеста занимается всегда именно суд первой инстанции) подлежит фиксированию посредством протокола только в двух случаях: при неявке в судебное заседание всех участников гражданского судопроизводства (но принятие апелляционной жалобы или протеста производится вне судебного заседания) или при отсутствии технической возможности вести звуко- или видеозапись (вряд ли, однако, в суде может отсутствовать возможность вести соответствующую запись абсолютно во всех случаях, когда имеет место подача апелляционной жалобы или протеста).

В-третьих, норма неверна и по существу. Принятие апелляционной жалобы (протеста) к производству – это властное волеизъявление суда правоприменительного характера, которое имеет важнейшее значение для развития апелляционного производства. Данное волеизъявление идентично акту возбуждения судом производства по делу по первой инстанции, т. е. акту принятия искового заявления (заявления) к производству. Но если возбуждение производства по делу по первой инстанции оформляется определением суда, то точно таким же образом должно быть оформлено и возбуждение апелляционного производства. Ни о каком использовании протокола здесь речи идти не может.

В этом плане весьма показательны правила ч. 2, 3 ст. 274 ХПК, которые, к сожалению, не были учтены разработчиками КГС: о принятии апелляционной жалобы (протеста) к производству суд апелляционной инстанции выносит определение, в котором указываются время и место проведения судебного заседания по рассмотрению апелляционной жалобы (протеста); определение суда о принятии апелляционной жалобы (протеста) к производству направляется лицам, участвующим в деле, не позднее пяти дней со дня поступления жалобы (протеста) в суд.

В ГПК и ХПК вопросы использования видео-конференц-связи для целей проведения судебных заседаний получили весьма фрагментарное регулирование. Так, соответствующие нормы разбросаны по всему тексту ГПК (см. п. 5 ч. 1 ст. 174, ч. 2 ст. 178, ст. 185–1, п. 9–1 ст. 262, ч. 6 ст. 267, ст. 419, ч. 4 ст. 428), ХПК (ч. 3 ст. 83, ч. 6 ст. 170, ст. 176–1, абз. 6 ч. 1 ст. 189–1) и оставляют без ответов многие сложные вопросы, касающиеся применения данного современного средства коммуникаций. В КГС же вопросы использования видео-конференц-связи получили гораздо более полное и системное регулирование. Так, КГС содержит специальную гл. 12 «Использование систем видео-конференц-связи в гражданском судопроизводстве», а также дефиницию самой видео-конференц-связи (п. 4 ст. 1).

В то же время дефиниция видео-конференц-связи не совсем верна. Согласно п. 4 ст. 1 КГС видео-конференц-связь – это способ осуществления процессуальных действий с использованием программно-технических средств передачи аудио- и видеоинформации по каналам связи в режиме реального времени. Однако, по нашему мнению, видео-конференц-связь – это не способ осуществления процессуальных действий, а способ коммуникаций суда и участников судопроизводств при совершении процессуальный действий в условиях, когда отдельные из участников судопроизводства находятся вне физической досягаемости состава суда (вне места его расположения).

Анализ содержащихся в КГС норм о видео-конференц-связи позволяет сделать вывод, что для дистанционных коммуникаций суда с участниками судопроизводства могут использоваться не любые технические устройства и технологии, а исключительно специально предназначенные для этого программно-технические средства, которыми оснащены суды. Иными словами, проведение видео-конференц-связи с помощью мобильного телефона судьи или участника судопроизводства недопустимо.

Правда, наряду с этим ч. 9 ст. 108 КГС предусматривает, что правила гл. 12 КГС не исключают возможности использования с согласия участвующих в деле лиц, которые присутствуют в судебном заседании, иных технических средств связи для фиксирования допроса свидетелей, объяснений участвующих в деле лиц, пояснений иных участников процесса, находящихся вне места расположения суда, рассматривающего дело.

Приведенная норма вызывает возражения по нескольким причинам. Во-первых, не совсем точно определена цель использования иных технических средств связи: они нужны не для фиксирования показаний, объяснений, пояснений (ведь фиксирование процесса осуществляется с помощью средств звуко-, видеозаписи или же протокола), а для их получения (восприятия, передачи). Во-вторых, отсутствие кон-

кретизации иных технических средств связи и регламента их применения способно привести к нарушению (ущемлению) процессуальных прав (интересов) участников судопроизводства, равно как и к неправильному разрешению дела по существу.

Новации в регулировании применения систем видео-конференц-связи сводятся в основном к следующим моментам:

– использование систем видео-конференц-связи возможно как по инициативе суда, так и по ходатайствам участвующих в деле лиц (ч. 1 ст. 108 КГС);

– с помощью систем видео-конференц-связи может быть проведено не только судебное заседание (в том числе предварительное) в целом, но и его часть (ч. 2 ст. 108 КГС), а также отдельное процессуальное действие вне судебного заседания (ч. 3 ст. 108 КГС);

– в судебном заседании при посредстве систем видео-конференц-связи могут совершаться абсолютно любые действия, в том числе проводиться исследование письменных, электронных и вещественных доказательств (ч. 4 ст. 108 КГС);

– применение систем видео-конференц-связи допустимо в судах всех инстанций: первой, апелляционной, кассационной и надзорной (ч. 5 ст. 108 КГС);

– предусмотрено новое, по сравнению с ч. 2 ст. 185–1 ГПК и ч. 2 ст. 176–1 ХПК, основание для отказа суда в применении систем видео-конференц-связи – «имеются иные обстоятельства, препятствующие использованию систем видео-конференц-связи» (п. 3 ч. 7 ст. 108 КГС), хотя в подобной абстрактной редакции норма не добавляет ясности в решение вопроса;

– в проведении сеанса видео-конференц-связи задействованы два суда: суд, рассматривающий дело (в нем находится состав суда с большинством участников судопроизводства), и суд, осуществляющий организацию видео-конференц-связи (в нем находится дистанционно коммуницирующий с составом суда участник (участники) судопроизводства); для организации сеанса видео-конференц-связи первый суд должен направить во второй суд соответствующее поручение (ч. 1 ст. 109 КГС);

– на участников судопроизводства, находящихся во втором суде, распространяются все правила судебного разбирательства (ч. 3 ст. 109 КГС), при этом действия, необходимые для обеспечения рассмотрения дела (проверка явки, установление личности и пр.), осуществляются в этом суде при содействии его судебного секретаря (ч. 4 ст. 109 КГС);

– если при использовании систем видео-конференц-связи полное, всестороннее и объективное исследование доказательств в судебном заседании невозможно или затруднительно, суд должен отложить разбирательство дела либо объявить в судебном заседании перерыв (ч. 6 ст. 109 КГС); правда, цели отложения разбирательства дела или объявления перерыва не определены: должен ли суд в период отложения или перерыва обеспечить явку тех лиц, которые участвовали в судебном заседании дистанционно, или получить в свое распоряжение доказательства, которые были дистанционно предъявлены этими лицами, или совершить какие-то иные действия;

– не позднее дня, следующего за днем проведения судебного заседания, из суда, который осуществлял организацию видео-конференц-связи, в суд, рассматривающий

дело, подлежат направлению не только представленные в судебном заседании доказательства, но и подтверждающие полномочия участвующих в деле лиц документы, полученные у свидетелей, экспертов, переводчиков подписки (ч. 7 ст. 109 КГС);

– сведения об использовании судом систем видео-конференц-связи должны быть указаны, помимо краткого протокола или протокола, также в итоговом судебном постановлении по делу (ч. 8 ст. 109 КГС).

Заключение. Проведенное исследование позволяет сделать следующие выводы:

– в КГС необходимо конкретизировать понятие «электронный документ», а также более системно урегулировать вопросы использования электронных документов;

– принятие судом первой инстанции апелляционной жалобы (протеста) к производству должно оформляться не протоколом, а путем вынесения судом соответствующего определения;

– в КГС требуется уточнить дефиницию видео-конференц-связи, а также регулирование некоторых вопросов применения данного способа коммуникаций; использование же любых иных средств связи для проведения судебных заседаний в дистанционном формате нуждается в подробных нормативных предписаниях.

Список литературы

1. Проект Кодекса гражданского судопроизводства Республики Беларусь // Правовой форум Беларуси. URL: https://forumpravo.by/publichnoe-obsuzhdenie-proektov-npa/forum15/16857-proekt-kodeksa-grazhdanskogo-sudoproizvodstva-respubliki-belarus (дата обращения: 05.09.2022).

2. Проект Кодекса гражданского судопроизводства Верховным Судом вынесен на общественное обсуждение // Национальный правовой интернет-портал Республики Беларусь. URL: https://pravo.by/novosti/novosti-pravo-by/2022/mart/69019/?fbclid=IwAR12pX4i85UY6Mqj3pGODp5hYEXj96mtQSFDMm77_ATuwMTOFd82nuMJHWw (дата обращения: 05.09.2022).

Н. Г. Соломина,
доктор юридических наук, доцент,
профессор кафедры гражданско-правовых наук,
Кузбасский институт Федеральной службы исполнения наказаний России;
профессор кафедры гражданского права,
Томский государственный университет систем управления
и радиоэлектроники

КРЕДИТНО-РАСЧЕТНЫЕ ПРАВООТНОШЕНИЯ С УЧАСТИЕМ ГРАЖДАН В УСЛОВИЯХ ЦИФРОВИЗАЦИИ БАНКОВСКОГО СЕКТОРА РОССИЙСКОЙ ЭКОНОМИКИ

Аннотация. В статье затрагивается вопрос недобросовестного использования участником профессиональной банковской деятельности онлайн-моделей

в работе с клиентами на стадии заключения и исполнения договоров кредитно-расчетной сферы. На примерах из судебной практики автор показывает, что клиент-гражданин в принципе лишен возможности защитить свои нарушенные интересы от недобросовестного поведения банка, активно использующего средства виртуального взаимодействия с клиентами.

Ключевые слова: цифровые правоотношения, онлайн-ресурсы, банковский продукт, договор присоединения, кредитный договор, форма договора, кешбэк

CREDIT AND SETTLEMENT LEGAL RELATIONS WITH THE PARTICIPATION OF CITIZENS IN THE CONDITIONS OF DIGITALIZATION OF THE BANKING SECTOR OF THE RUSSIAN ECONOMY

Abstract. The article addresses the issue of unfair use by a participant in professional banking of online models in working with clients at the stage of concluding and executing credit and settlement agreements. Using examples from judicial practice, the author shows that a client-citizen is basically deprived of the opportunity to protect his violated interests from the unscrupulous behavior of a bank actively using the means of virtual interaction with clients.

Keywords: Digital legal relations, Online resources, Banking product, Accession agreement, Loan agreement, Contract form, Cashback

Сегодня уже никого не удивишь тем, что взаимоотношения клиента – физического лица и банка выстраиваются без непосредственного контакта глаза в глаза. Используя онлайн-ресурсы, граждане вступают в банковские договорные правоотношения, не задумываясь порой о рисках, которые обусловлены использованием электронного (цифрового) формата общения с контрагентом – субъектом профессиональной деятельности, для которого последняя является основным источником дохода. Поэтому надеяться на то, что предлагаемые отечественными банками «новые» онлайн-модели работы с клиентами (а равно «новые» банковские продукты) будут выгодны исключительно клиентам, большое заблуждение.

Отечественные банки внедряют в свою деятельность оправдавшие себя в мировой банковской практике онлайн-модели работы с клиентами. Назначение этих моделей одно: увеличить прибыль банка в отсутствие какой-либо опасности понести убытки. При правильной организации работы по продвижению «нового» банковского продукта в массы в руках банка оказывается огромное количество клиентов-потребителей, рассчитывающих на получение выгоды. Так, например, по содержанию рекламы, связанной с выпуском дебетовых карт Tinkoff Black, банк «Тинькофф» обещает клиентам не только бесплатное обслуживание этой карты, но и то, что это обслуживание «навсегда». И это предлагает банк, который на рынке финансовых услуг работает всего полтора десятка лет. Чтобы понять, что подобный маркетинговый ход является лишь уловкой, достаточно знать, что на сегодняшний день нет такого банковского продукта, который характеризовался бы признаком «бесконечности» существования, в том

числе с точки зрения стабильности условий его предоставления. И причина не в том, что любой банк может лопнуть. Кредитно-расчетная сфера развивается семимильными шагами, в том числе с позиции способов совершения безналичных расчетов. Это сегодня банковские карты выступают популярным и удобным инструментом расчетов. А завтра, с учетом развития технического прогресса, они будут восприниматься в качестве анахронизма наравне с кассетным магнитофоном и кнопочным сотовым телефоном. Иначе говоря, наступит время, когда банки откажутся от предоставления такого рода банковского продукта по той или иной причине.

Основываясь на практике отдельных отечественных банков, обозначим некоторые аспекты внедрения цифрового формата в кредитно-расчетные отношения, которые, на наш взгляд, вряд ли можно отнести к достоинствам цифровизации банковского сектора экономики с позиции учета интересов клиента – физического лица.

Участие физического лица на стороне клиента по договорам кредитно-расчетной сферы, предметом которых выступает тот или иной банковский продукт, накладывает отпечаток как на специфику установления договорных связей, так и на природу возникших договорных правоотношений – такие правоотношения приобретают качество потребительских (что, в свою очередь, позволяет применять к ним законодательство о защите прав потребителей). Что касается специфики установления договорных связей, то она в первую очередь выражается в том, что заключение любого банковского договора с участием гражданина-потребителя происходит по модели договора присоединения (ст. 428 ГК РФ). Применение этой модели в банковском секторе экономики обусловлено характером профессиональной деятельности банка: он совершает одинаковые по своему содержанию сделки, что исключает необходимость каждый раз согласовывать условия договора с любым обратившимся к нему потребителем. Нет такой необходимости и у потребителя: он исходит из того, что условия банковской сделки будут если и не такими же, то, по крайней мере, не сильно отличающимися от аналогичных сделок, совершаемых в отношении любого другого гражданина, потребляющего банковский продукт. Заключение договора на заранее объявленных условиях всегда предполагает добросовестность поведения субъекта профессиональной деятельности – банка. На случай, если поведение такого субъекта не будет соответствовать масштабу добросовестного поведения с точки зрения «качества» условий договора присоединения (даже если внешне такой договор не противоречит закону и иным правовым актам), закон предоставляет присоединившейся стороне весьма весомое охранительное средство – она вправе требовать изменения или расторжения договора. Общую границу масштаба добросовестного поведения банка можно обозначить законодательной установкой – «недопустимость включения в договор явно обременительных для присоединяющейся стороны условий, которые она, исходя из своих разумно понимаемых интересов, не приняла бы при наличии у нее возможности участвовать в определении условий договора».

На первый взгляд, указанное охранительное средство выглядит оптимальным и достаточным для защиты интересов присоединяющейся стороны. Однако

что делать, если на стадии заключения договора потребитель лишен возможности адекватно оценить содержание будущего договора по причине чрезмерно большого числа договорных условий? Тем более что банк предлагает ему ознакомиться с этим договором, а впоследствии и заключить его, используя исключительно формат онлайн-общения. Так, например, АО «Альфа-Банк» отказалось от разработки стандартных договоров применительно к каждому конкретному банковскому продукту, а разработало один договор о комплексном банковском обслуживании физических лиц [1]. При присоединении к этому договору клиент может воспользоваться любым банковским продуктом (получить банковскую карту, открыть банковский счет, взять кредит, открыть депозит и т. д.). Данный договор существует в формате pdf-документа, содержание которого изложено на 222 страницах с тарифами по всем банковским продуктам, изложенными еще на 295 страницах. То есть весь договор в целом составляет 517 страниц (!). Даже несведущему в юриспруденции лицу очевидно, что содержание предлагаемого к заключению договора чрезмерно велико. Согласно п. 2.1.2 договора о комплексном банковском обслуживании физических лиц клиент заключает договор путем предоставления банку подтверждения о присоединении к условиям договора, в частности, в электронном виде с подписанием договора простой электронной подписью, в том числе в интернет-канале. Правда, прежде чем воспользоваться этим способом заключения договора, клиент должен принять условия еще одного договора – соглашения об электронном документообороте. Идентификация клиента, желающего получить той или иной банковский продукт, происходит посредством введения секретного кода, за счет которого и происходит формирование простой электронной подписи. Банк, получивший запрос клиента, подтвержденный простой электронной подписью, предоставляет ему соответствующий банковский продукт. В итоге клиент, которому противостоит огромная армия мошенников, специализирующихся на электронном документообороте, загоняет себя в весьма неудобную ситуацию: в случае получения банковского продукта любые возражения клиента банка о том, что его секретным кодом воспользовался кто-то другой, для банка не имеют значения.

Так, в одном из споров клиент АО «Альфа-Банк» просил суд признать ничтожным кредитный договор, ссылаясь на то, что он его не подписывал, а соответственно, не мог получить кредит [2]. Вместе с тем как установил суд, истец (клиент банка) через онлайн-ресурс обратился в АО «Альфа-Банк» с анкетой-заявлением на получение кредитной карты. После получения ключа простой электронной подписи на номер своего мобильного телефона, клиент (используя ключ) подписал договор о комплексном банковском обслуживании физических лиц и обратился в банк с заявлением об открытии счета, выдаче кредитной карты. Через некоторое время клиент, воспользовавшись приложением «Альфа-Мобайл», направил заявление на получение кредита наличными в размере 468 000 рублей под 14,4 % годовых. Все документы, исходящие от клиента, в том числе кредитный договор, были подписаны простой электронной подписью – путем ввода корректного кода, который поступил на принадлежащий истцу номер телефона. Отказывая в удовлетворении требования истца, суд исходил

из того, что сторонами согласованы все существенные условия кредитного договора, соблюдена его форма, а значит, отсутствуют основания для признания договора ничтожным. Ссылку истца на то, что в отношении него были совершены мошеннические действия, в результате которых он передал секретный код третьим лицам, заключившим кредитный договор и обналичившим сумму кредита, суд не принял во внимание.

Данный пример показывает, что процесс заключения договора в сфере кредитно-расчетных отношений с использованием онлайн-ресурсов не может быть сведен к упрощенной процедуре кодирования простой электронной подписи клиента, которой можно подписать любой электронный документ. Процедура персонификации при совершении банковских сделок в виртуальном пространстве должна быть максимально приближена к процедуре заключения договора глаза в глаза, что, в свою очередь, предполагает установление на уровне банковского законодательства специального способа достоверного определения лица (клиента банка), выразившего волю на совершение банковской сделки посредством использования электронных каналов связи.

Что касается объема договора, предлагаемого к заключению, то практика АО «Альфа-Банк» не является исключением. Сегодня подобные договоры о комплексном обслуживании клиентов разработаны и другими банками. Например, АО «Россельхозбанк» при заключении индивидуального соглашения о кредитовании счета оговаривается, что его неотъемлемыми частями являются ряд приложений, а именно: «Условия комплексного банковского обслуживания держателей карт АО «Россельхозбанк» [3] (размер данного документа составляет 64 страницы), «Тарифный план «Карта Хозяина», «Дебетовая карта Хозяина».

В одном из судебных дел клиенту после подписания соглашения о кредитовании счета (со всеми причитающимися приложениями) были выданы карты, к каждой из которых была подключена дополнительная опция CashBack согласно тарифным планам; через некоторое время клиент перестал получать возврат денежных средств на карты, что и послужило основанием обращения в суд [4]. Суд, отказывая в удовлетворении требования, исходил из того, что начисление суммы CashBack является правом банка. Так, согласно условиям комплексного банковского обслуживания держателей карт, банк имеет право изменять условия такого обслуживания, а также тарифы с уведомлением держателя в установленном этими же условиями порядке. Что касается порядка уведомления клиента об изменении условий обслуживания, то банк предусмотрел для себя ряд альтернативных способов информирования клиента, среди которых размещение информации на веб-сайте банка в сети Интернет. Более того, этими же условиями предусмотрено, что в целях обеспечения своевременного получения информации об изменении условий обслуживания и тарифов именно на держателя карты возлагается обязанность самостоятельно получать сведения об изменениях, которые планирует внести банк. Суд не воспринял данные условия договора в качестве обременительных, указав: «Подписав Соглашение и заявку на открытие счета, клиент подтверждает, что им до заключения договора получена вся необходимая информация

об услугах, тарифах, порядок изменений Условий и тарифов. Все документы являются общедоступными, размещаются в местах оформления банковских продуктов и на сайте АО “Россельхозбанк”».

Что помешало суду признать эти условия в качестве явно обременительных и защитить права клиента (присоединившейся стороны) по правилам п. 2 ст. 428 ГК РФ, в частности изменить условия комплексного банковского обслуживания держателей карт АО «Россельхозбанк»? Причина, скорее всего, кроется в той банковской практике, которая сложилась на сегодняшний день относительно предоставления банковских продуктов, в том числе в рамках соглашений о комплексном обслуживании клиентов: наличие явно обременительных условий в договорах кредитно-расчетной сферы приобрело массовый характер; признать явно обременительными условия договора – значит признать недобросовестной всю существующую практику разработки договорных условий в банковском секторе экономики.

Список литературы

1. Официальный сайт АО «Альфа-Банка». URL: https://alfabank.ru/retail/tariffs/ (дата обращения: 14.07.2022).

2. Определение Седьмого кассационного суда общей юрисдикции от 05.05.2022 дело № 88–7982/2022 // Официальный сайт Седьмого кассационного суда общей юрисдикции. URL: http://7kas.sudrf.ru (дата обращения: 14.07.2022).

3. URL: https://www.rshb.ru/download-file/298018/ (дата обращения: 14.07.2022).

4. Определение Четвертого кассационного суда общей юрисдикции от 29.03.2022 дело № 88–9128/2022 // Официальный сайт Четвертого кассационного суда общей юрисдикции. URL: http://http://4kas.sudrf.ru (дата обращения: 14.07.2022).

Г. В. Станкевич,
доктор политических наук, кандидат юридических наук, доцент,
Ставропольский филиал Московского педагогического
государственного университета

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ФУНКЦИОНИРОВАНИЯ БЕЗНАЛИЧНЫХ РАСЧЕТОВ В УСЛОВИЯХ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассматривается современное состояние алгоритма совершения безналичных расчетов, выявляются актуальные проблемы и перспективы их решения на законодательном и правоприменительном уровнях; раскрывается роль банковского регулятора в процессе развития национальной платежной системы, возможности расширения сфер применения цифровых финансовых активов и механизмов их защиты от мошеннических действий. Уделяется внимание роли и значению цифровых технологий в расширении электронной системы платежей и системы быстрых платежей, сокращении наличного оборота.

Ключевые слова: гражданское право, банковское право, безналичные расчеты, национальная платежная система, цифровые технологии, кредитные организации, система быстрых платежей

ACTUAL PROBLEMS OF FUNCTIONING OF NON-CASH PAYMENTS IN THE CONDITIONS OF APPLICATION OF DIGITAL TECHNOLOGIES

Abstract. The article examines the current state of the algorithm for making non-cash payments, identifies current problems and prospects for their solution at the legislative and law enforcement levels; reveals the role of the banking regulator in the development of the national payment system, the possibility of expanding the scope of digital financial assets and mechanisms to protect them from fraud. Attention is paid to the role and importance of digital technologies in expanding the electronic payment system and the system of fast payments, reducing cash turnover.

Keywords: Civil law, Banking law, Non-cash settlements, National payment system, Digital technologies, Credit organizations, Fast payment system

Введение. Устойчивая национальная платежная система имеет ключевое значение для финансового благополучия государства. Политические изменения внутри и за пределами нашей страны, международная обстановка в целом, мировой экономический кризис и другие факторы оказывают прямое влияние на нашу экономику.

Глобализация и цифровизация затрагивают финансовый сектор, и зачастую государство не может полностью контролировать и влиять на эти процессы. Национальные экономики ряда стран зависят друг от друга и поэтому уязвимы. Нередко страны используют свое монопольное положение в целях давления на неугодное государство, и в основном страдает экономика. Наглядным примером могут являться продолжающиеся санкции против России.

Экономическая политика государства должна быть направлена на минимизацию предполагаемых издержек глобализации.

На устойчивость национальной платежной системы (далее – НПС) влияет состояние отечественной банковской системы. События, происходящие в нашей стране и в мире, невнимание и ошибочные действия властей в отношении финансовой системы способны привести банковскую систему к кризису. В такой обстановке России необходимо проводить эффективную политику по обеспечению экономической безопасности государства, особенно с развитием цифровых активов. Федеральный закон от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации» призван укрепить экономическую безопасность посредством установления основ стратегического планирования, включая меры, направленные на социально-экономическое развитие государства, и сроки для реализации указанных мер [1].

Основная часть. Существенным пластом проблем, возникающих в функционировании НПС, являются риски системы расчетов, которые подрывают осуществление бесперебойных и своевременных платежей.

Например, операционный риск встречается как в самой кредитной организации, так и в платежной системе. Рассматриваемый риск может наступить в ре-

зультате непрофессионализма служащих банка, ошибок проведения банковских операций, сбоев и недостатков в информационных, технологических и иных системах, а также в ходе внешнего воздействия. Все эти проблемы приводят к задержкам осуществления расчетов и системным рискам.

Кредитные организации в соответствии с письмом Банка России от 24.05.2005 № 76-Т «Об организации управления операционным риском в кредитных организациях» (далее – Письмо Банка России № 76-Т) разрабатывают систему управления операционными рисками, которая содержит комплекс организационных, методических и информационных средств, направленных на «выявление, оценку, мониторинг, контроль и (или) минимизацию операционного риска» [4].

Банк России разрабатывает меры по обеспечению устойчивости банковской системы. Он устанавливает определенные требования к кредитным организациям и следит за их соблюдением, предлагает рекомендации и меры по управлению банковскими рисками.

Существует принцип «Знай своего клиента», согласно которому до приема на обслуживание кредитная организация обязана идентифицировать клиента, его представителя или выгодоприобретателя [1]. Кредитным организациям запрещается обслуживать анонимные счета, все это делается в целях противодействия отмыванию доходов и финансированию терроризма.

Также существует принцип «Знай своего служащего», в рамках которого рекомендуется уделять внимание квалификации персонала, доводить до сведения работников должностные инструкции, проводить курсы повышения квалификации, также учитывать «личностные характеристики служащих применительно к содержанию и объему выполняемой работы и мере ответственности» [5].

Согласно ст. 15 Закона № 161-ФЗ, надзор и наблюдение в НПС осуществляет Банк России, целями которых является обеспечение стабильности НПС и ее дальнейшее развитие, а также защита интересов вкладчиков и кредиторов [3]. Банк России контролирует соблюдение организациями, осуществляющими операции с денежными средствами, требований законодательства о НПС и других нормативных актов Банка России.

Однако активный банковский надзор в условиях применения цифровых технологий не позволяет решить существующие проблемы функционирования платежной системы. Для передачи финансовых сообщений используется система SWIFT. Данная система имеет как преимущества, так и недостатки. SWIFT является мировым монополистом в своей сфере, созданная на основе европейского законодательства, она защищает интересы западных участников. Также доступ к этой системе получила сверхдержава, которая активно настаивала на отключении России от рассматриваемой системы, и крупнейшие банки Россию отключили от SWIFT. Теперь российские банки не могут обмениваться финансовыми сообщениями с заграничными контрагентами, последствие – невозможность проведения безналичных расчетов с иностранными партнерами.

В противовес этой системе Указанием Банка России от 05.10.2015 № 3814-У «О порядке оказания Банком России услуг по передаче финансовых сообщений кредитным организациям и их клиентам – юридическим лицам» [6]в 2015 г. была создана и начала функционировать система передачи финансовых сообщений (далее – СПФС).

СПФС не позволяет переводить денежные средства за границу и не работает в ночное время, тем самым уступая западному конкуренту, поэтому ранее ее использовали как запасную систему, продолжая пользоваться SWIFT [18]. А в условиях санкций СПФС на современном этапе – единственно возможный способ передачи финансовых сообщений. СПФС имеет плюсы, такие как защита системы от внешнего воздействия, низкие тарифы, ускорение обмена сообщениями.

Те же события, что подтолкнули Банк России к запуску СПФС, стали толчком для создания национальной системы платежных карт (НСПК) и эмиссии платежных карт «Мир». На нормативно-правовом уровне для регулирования этой системы и подчеркивания ее национального статуса поправками в Закон № 161-ФЗ была добавлена гл. 4.1 о НСПК.

До создания оператора НСПК такие платежные системы, как Visa и MasterCard, практически были монополистами на российском рынке платежных карт, они диктовали свои условия и преследовали собственные интересы, действуя без особых ограничений. Также многочисленная информация при проведении безналичных расчетов передавалась в процессинговый центр, находящийся вне территории РФ.

Сегодня все операции по картам Visa и MasterCard проходят через центр обработки информации НСПК, и это касается только транзакций внутри РФ.

В соответствии с п. 12 ст. 16 Закона № 161-ФЗ операторам платежной инфраструктуры запрещено передавать информацию по проведению безналичных расчетов за границу, также они не могут в одностороннем порядке приостановить или прекратить «оказание услуг платежной инфраструктуры участникам платежной системы и их клиентам».

В результате применения этих мер платежи россиян защищены от зарубежного вмешательства, а информация по ним не выйдет за пределы РФ.

Проблемы с картой «Мир» в основном сводятся к тому, что ее мало где можно использовать за рубежом. На законодательном уровне эта проблема не решается, ведь законы России живут на территории России, поэтому НСПК заключает соглашения о выпуске кобейджинговых карт с другими международными платежными системами (хотя, например, общие положения о договоре и выбор сторонами права, которое подлежит применению к их правам и обязанностям по этому договору, регулируется Гражданским кодексом РФ). На сегодняшний день эмитируются карты «Мир-Maestro», «Мир-JCB», «Мир-UnionPay» [17. С. 329–335].

Кобейджинговые карты в России используются как карты «Мир», а в иностранном государстве – по правилам соответствующих международных платежных систем.

Россия ведет переговоры с зарубежными странами (в основном со странами ЕАЭС) о взаимном сотрудничестве, чтобы карты «Мир» принимали за границей. Ограниченный круг операций доступен на территории 14 стран: Беларуси, Узбекистана, Казахстана, Турции и др.

Среди проблем в функционировании национальной платежной системы граждане часто сталкиваются с рисками платежных инструментов. Банковские карты являются самым распространенным средством оплаты, но, несмотря на все «плюшки», которые получают владельцы карт, с этим платежным инструментом связано немало проблем.

Первый существенный недостаток – это безопасность. Да, банковские карты оснащены системой безопасности, но она до сих пор до конца не проработана. Для покупки товара в интернет-магазине иногда достаточно знать реквизиты, которые указаны на самой карте. Подтверждения платежа в ряде случаев не требуется, наступает момент окончательности перевода денежных средств, и зачастую очень проблематично вернуть свои денежные средства в случае незаконного списания.

Денежные средства могут списать из-за технического сбоя или противоправных действий работника банка, который воспользовался своим служебным положением, и ответственность за это в соответствии с ГК РФ будет нести банк.

Злоумышленниками на основе цифровых технологий разработано бесчисленное множество способов мошенничества с банковскими картами (кардинг). Мошенники устанавливают на банкоматы (терминалы) скиммер, устройство, считывающее персональные данные с магнитной полосы карты. Используют скрытую видеокамеру или накладную клавиатуру. Все эти способы применяются для кражи банковских реквизитов.

В первую очередь владелец банковской карты сам осуществляет меры предосторожности, чтобы ценная информация не была похищена. Кредитные организации советуют не вводить PIN-код на сомнительных устройствах, быть бдительными при использовании банкоматов и, если произошли разнообразные технические сбои, немедленно обратиться в банк.

Если же средства все-таки были незаконно списаны, используется процедура chargeback – возврат платежа по спорной трансакции. В законодательстве РФ эта процедура оспаривания платежа не описана. Она применяется в целях минимизации мошенничества и повышения у банковских клиентов доверия к расчетам, но перед ее применением следует попытаться урегулировать это проблему с торгово-сервисной организацией, и если эта попытка не принесет положительных результатов, то после этих действий можно воспользоваться процедурой chargeback (что и описано в операционных правилах Visa).

Рассматриваемая процедура предусмотрена во многих платежных системах. Владелец карты, с которой были незаконно списаны деньги, подготавливает претензию о спорной операции, банк-эмитент решает, начинать процедуру или нет. Если банк-эмитент принимает решение о начале процедуры, он направляет эквайеру соответствующее уведомление о начале процедуры.

Эквайер сам решает, привлекать ли торгово-сервисную организацию или же самостоятельно провести chargeback, если сочтет претензию владельца карты обоснованной.

По итогам проведения процедуры клиенту могут быть возвращены его денежные средства. При отрицательном исходе процедуры банк-эмитент возвращает клиенту его претензию, после этого тот вправе обратиться в суд [16. С. 58–69].

Целесообразно включить в Закон № 161-ФЗ содержание процедуры chargeback и ключевые принципы ее проведения в целях внесения ясности и единообразия в проведение данной процедуры.

При использовании интернет-банкинга самым распространенным способом похищения персональных данных является фишинг, вредоносный веб-сайт, где

потенциальную жертву фишинга просят ввести персональные данные с целью хищения. В мобильном банкинге мошенники атакуют само мобильное устройство, заражая его вредоносными программами или вовсе похищая смартфон.

Применяются разнообразные методы защиты от фишинга, в том числе законодательные меры борьбы с ним. Махинации с деньгами, пусть они и проводятся в Интернете, рассматриваются как мошенничество. Жертва фишинга, если будет найден предполагаемый создатель вредоносного сайта, может подать на него в суд и требовать возмещения причиненных убытков в соответствии со ст. 15 ГК РФ. Также к злоумышленникам применяются меры административной и уголовной ответственности (например, ст. 7.27 КоАП РФ, гл. 28 УК РФ полностью посвящена преступлениям в сфере компьютерной информации).

Банки рекомендуют своим клиентам в первую очередь тщательно проверять адрес сайта и не вводить свои персональные данные на не заслуживающих доверия ресурсах, а также установить антивирус на гаджеты.

Проблемами в осуществлении бесконтактных платежей является ограниченное количество терминалов с поддержкой NFC-технологий. В целом данный вид платежей обладает повышенной безопасностью.

Что касается криптовалюты, основными проблемами ее являются плавающий курс и децентрализация эмиссии [14. С. 33–45]. Криптовалюта не является законным средством платежа, расчеты с ее участием осуществляются на свой страх и риск.

Трансакции анонимны и сложны для контроля, поэтому у государства есть опасения, что пользователи пытаются скрыться от налогообложения, или, еще хуже, уйти в теневой сектор, финансировать терроризм.

Государство стремится к контролю за криптовалютами, пытается упорядочить процесс их обращения. В Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» определен статус криптовалюты: не является средством платежа в России. Этот закон регулирует отношения по выпуску, учету и обращению цифровых финансовых активов, а также деятельность операторов информационной системы, где рассматриваемые активы выпускаются и обмениваются.

Проблемы в правовом регулировании на сегодняшний день создают множество трудностей участникам безналичных расчетов. Эти проблемы преобразуются в многочисленные судебные разбирательства.

В ГК РФ содержатся понятия форм и общие правила проведения безналичных расчетов, но определение «безналичных денежных средств», с помощью которых эти расчеты осуществляются, отсутствует.

Законодатель рассматривает их как «денежные средства, находящиеся на банковском счете», «остаток денежных средств», говорит о расчетах в «безналичном порядке». В ст. 128 ГК РФ впервые появляется термин «безналичные денежные средства», но легального определения этому термину опять-таки нет. В этой статье интересно то, что законодатель причисляет наличные деньги к вещам, а безналичные денежные средства – к категории «иное имущество».

В ст. 29 Закона № 86-ФЗ сказано, что единственным легальным средством наличного платежа на территории РФ являются банкноты и монеты, выпущенные

Центральным банком РФ. По замыслу ст. 140 ГК РФ безналичные деньги, посредством которых осуществляются безналичные расчеты, тоже являются законным средством платежа наряду с наличными деньгами.

Относительно юридической природы безналичных денежных средств цивилистами выдвигались различные точки зрения, зачастую противоположные друг другу: вещно-правовая природа безналичных денег [12. С. 236] и как право требования клиента к банку, которое носит обязательственный характер [11. С. 4–5]. Таким образом, цивилисты не пришли к единому мнению касательно правовой природы безналичных денежных средств. Такие разные подходы вызывают споры о том, какие нормы ГК РФ следует применять к расчетам.

Полагается, что законодатели разрешили этот спор, ведь гл. 46 ГК РФ о расчетах находится в разделе IV «Отдельные виды обязательств» ГК РФ.

Рассмотрим ситуацию, когда денежные средства клиент по ошибке перевел не на тот счет. Если решать этот вопрос с позиции вещного права, то иск будет направлен лицу, которому ошибочно были зачислены денежные средства. Если рассматривать этот вопрос с позиции обязательственного права, то тут ситуация будет решаться на основании договора банковского счета между клиентом и банком.

Следует внести изменения в ГК РФ, дополнив ст. 140 ГК РФ дефиницией «безналичные денежные средства», окончательно разрешив споры между цивилистами (а также между правоприменителями).

Анализ законодательства позволил выявить проблему касаемо исчисления сроков при проведении безналичных расчетов. По логике ст. 849 ГК РФ банк обязан зачислять на счет клиента, выдавать или списывать по его распоряжению денежные средства «не позднее дня, следующего за днем поступления в банк соответствующего платежного документа», если не установлено иное (статья не охватывает межбанковские расчеты).

Ст. 31 ФЗ № 395–1 устанавливает аналогичные ст. 849 ГК РФ сроки для кредитных организаций, но говорит только о перечислении и зачислении средств на счет клиента, также применяет термин «операционный день», что тоже подразумевает ст. 849 ГК РФ, но не указывает.

И, наконец, п. 5 ст. 5 Закона № 161-ФЗ устанавливает сроки перевода денежных средств – три рабочих дня с момента списания со счета плательщика денежных средств, (если перевод без открытия банковского счета, моментом списания считается день, когда плательщик предоставил наличные деньги банку).

В этом случае нормы ГК РФ и ФЗ № 395–1 аналогичны друг другу (в части сроков зачисления и перечисления), но по-разному оформлены. Срок для операций составляет два операционных дня, включая день поступления распоряжения в банк.

Непонятно, как взаимодействует с этими статьями п. 5 ст. 5 Закона № 161-ФЗ. Из текста этой статьи следует, что она устанавливает сроки перевода денежных средств, выдача и зачисление туда не входят. Также статья различается моментом начала исчисления сроков. «При этом под списанием логично понимать именно совершение банком расходной операции по счету, а не предоставление клиентом соответствующего распоряжения в банк», – пишет О.А Тарасенко [15. С. 46–54]. Выходит, эта статья устанавливает срок для межбанковских расчетов по корреспондентским счетам.

Также рассматриваемые статьи не учитывают различные формы безналичных расчетов, для которых установлены иные сроки. Например, при расчетах по инкассо или по аккредитиву совершаются действия, не связанные с перечислением средств (например, предъявление платежных требований для акцепта).

Судебная практика сталкивается с проблемой неправильного толкования сторонами судебного разбирательства сроков исполнения инкассового поручения. В соответствии с Информационным письмом Президиума ВАС РФ от 15.01.1999 № 39 «при определении срока проведения инкассовых операций суд учитывает особенности их проведения» [7].

Получается, при определении срока исполнения распоряжения следует учитывать три рассматриваемые статьи, форму безналичных расчетов и положения договора банковского счета, если там установлены иные сроки.

Следует внести конкретику в ст. 849 ГК РФ и ст. 31 ФЗ № 395–1 и унифицировать эти статьи для устранения проблем в толковании.

За нарушение сроков банк можно привлечь к ответственности и потребовать выплатить неустойку по ст. 856 ГК РФ или уплатить проценты по ст. 866 ГК РФ (также к расчетным отношениям применяются положения главы 25 ГК РФ).

Не урегулирован полностью вопрос об ответственности банка перед клиентом за списание денежных средств со счета клиента по распоряжению неуполномоченного лица. Некоторые суды до сих пор взваливают вину за несанкционированное списание на клиентов, чьи средства были похищены. Еще в п. 2 Постановления Пленума ВАС от 19.04.1999 № 5 было установлено, что ответственность за это возлагается на банки, если в законе и договоре банковского счета не установлено иное [8] (такое же мнение было выражено в Определении СК по гражданским делам Верховного Суда РФ от 10.01.2017 № 4-КГ16–66). Речь идет и о тех ситуациях, когда банк не сумел установить, что исполняет распоряжение неуполномоченного лица. Но в таких ситуациях следует обращать внимание на действия клиента, если он своими действиями способствовал несанкционированному списанию средств со своего счета, ответственность можно уменьшить (п. 2 ст. 404 ГК РФ).

Получается, банк несет ответственность на незаконное списание денежных средств со счета с использованием дистанционных сервисов обслуживания.

Но такое положение дел будет нарушать принцип равенства сторон в договорных отношениях (п. 1 ст. 1 ГК РФ), ведь даже если банк осуществил соответствующие процедуры по приему распоряжения, произвел идентификацию клиента, он все равно будет привлекаться к ответственности, такой подход ставит банки в невыгодное положение.

Целесообразно дополнить ст. 856 ГК РФ п. 2, где будет закреплено, что банк несет ответственность за несанкционированное списание средств со счета клиента, если оно было совершено по распоряжению неуполномоченного лица, в этом случае банк должен вернуть клиенту списанную сумму в полном объеме, проценты по ст. 852 ГК РФ. Но в ситуациях, когда банк не сумел установить, что исполняет распоряжение неуполномоченного лица; надлежащим образом выполнял процедуры, установленные законом, банковскими правилами и договором банковского счета, а также если клиент не был осмотрительным и тем самым способ-

ствовал несанкционированному списанию средств со своего счета и все это будет установлено в надлежащем порядке – необходимо уменьшить размер ответственности (п. 2 ст. 404 ГК РФ).

Момент исполнения денежных обязательств при безналичных расчетах, как и сроки осуществления безналичных расчетов, будет зависеть от конкретной формы расчетов.

Доминирует позиция, по которой моментом исполнения денежных обязательств по замыслу ст. 316 ГК РФ (данная статья рассматривает место исполнения денежных обязательств), что подтверждается Постановлением Пленума ВС РФ от 22.11.2016 № 54 (Решением АС Новосибирской области от 27.11.2018 по делу № А45–38505/2018), считается зачисление средств на корсчет банка, обслуживающего кредитора (или банка-кредитора по отношению к плательщику) [9].

Однако необходимо принять во внимание, что если должник и кредитор обслуживаются одним банком, то моментом исполнения денежного обязательства будет считаться зачисление соответствующей суммы на счет кредитора. Все это действует для расчетов платежными поручениями, аккредитивами и чеками, но совершенно не подходит для расчетов по инкассо.

Если рассматривать общепринятое мнение, то моментом исполнения денежных обязательств при расчетах по инкассо считается своевременное списание денежных средств со счета плательщика. В этой части ГК РФ был приведен в порядок в соответствии с Унифицированными правилами по инкассо.

Ст. 316 ГК РФ отражает пространственную модель места исполнения обязательства, ведь темпоральная модель, которая определяет момент исполнения обязательства, имеет недостаток. Например, если должник исполнит обязательство в надлежащий момент, но ошибочно переведет деньги на другой счет кредитора, находящийся в обанкротившемся банке. Если бы в ст. 316 ГК РФ была закреплена темпоральная модель, обязательство должника перед кредитором считалось бы исполненным. Пространственная модель посчитает такое исполнение ненадлежащим, что подтверждает Постановление Президиума ВАС РФ от 30.07.2013 № 1142/13. Министерство обороны РФ ошибочно перечислило долг по государственному контракту на расчетный счет «НПЦ Спецоснащение МО», открытый в АКБ «Лефко-банк», у которого была отозвана лицензия. До ошибочного перевода стороны заключили дополнительное соглашение, в котором банковские реквизиты «НПЦ Спецоснащение МО» были изменены. Поэтому Президиум ВАС РФ справедливо посчитал, что риски банкротства АКБ «Лефко-банк» возлагаются на министерство, которое не учло измененные реквизиты [10].

С учетом изложенного можно сделать следующие выводы. На современном этапе наличные деньги постепенно исчезают из оборота, их доля в денежной массе на начало 2021 г. – 25,7 %. Доля безналичных расчетов, наоборот, растет из года в год, количество трансакций в 2021 году выросло до 74,3 %, создается инфраструктура, которая наполняет рынок все новыми товарами и услугами. Безналичные расчеты все чаще используются гражданами в повседневной жизни, доверие населения растет.

Распространению безналичных расчетов способствует платежная система Банка России и частные платежные системы. Платежная система ЦБ РФ являет-

ся самой масштабной по территориальному охвату – целых девять часовых зон! Переводы осуществляются с помощью систем БЭСП, ВЭР и МЭР, СБР, СБП.

Пополняется рынок электронных средств платежа, самыми популярными считаются платежные карты и электронные кошельки. ЭСП удобны в использовании и значительно упрощают безналичный оборот, снижают стоимость услуг по переводу денежных средств. Сегодня рынок перенесся в информационно-телекоммуникационную систему «Интернет», где с помощью ЭСП, СБП можно купить билет на самолет или оплатить проезд в метро.

Заключение. В НПС присутствует множество проблем, на ее устойчивость влияют как внешние, так и внутренние факторы. Среди проблем в функционировании национальной платежной системы обычно преобладают риски системные и платежных инструментов.

Выявлены проблемы в правовом регулировании, такие как отсутствие в гражданском законодательстве дефиниции «безналичных денежных средств», проблемы исчисления сроков и др. Необходимо внести изменения в конкретные статьи ГК РФ и в законодательство, затрагивающее осуществление безналичных расчетов.

Чтобы оперативно реагировать на актуальные проблемы, национальная платежная система должна быть организационно-устойчивой, в том числе должно происходить совершенствование законодательства в сфере безналичных расчетов, все это необходимо для выполнения ключевой цели НПС – проведения бесперебойного и своевременного исполнения платежей. Дальнейшее совершенствование НПС будет благоприятно влиять как на развитие безналичных расчетов, так и на процветание всей финансовой системы.

Список литературы

1. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Российская газета. 2001. 9 августа.

2. Федеральный закон от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации» // Российская газета. 2014. 3 июля.

3. Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 14.07.2022) «О национальной платежной системе» // Российская газета. 2011. 30 июня.

4. Письмо Банка России от 24.05.2005 № 76-Т «Об организации управления операционным риском в кредитных организациях» // Вестник Банка России. 2005. № 28.

5. Письмо Банка России от 30.06.2005 № 92-Т «Об организации управления правовым риском и риском потери деловой репутации в кредитных организациях и банковских группах» // Вестник Банка России. 2005. № 34.

6. Указание Банка России от 05.10.2015 № 3814-У «О порядке оказания Банком России услуг по передаче финансовых сообщений кредитным организациям и их клиентам – юридическим лицам» // Вестник Банка России. 2015. № 112.

7. Информационное письмо Президиума ВАС РФ от 15.01.1999 № 39 «Обзор практики рассмотрения споров, связанных с использованием аккредитивной и инкассовой форм расчетов» // Вестник ВАС РФ. 1999. № 4.

8. Постановление Пленума ВАС РФ от 19.04.1999 № 5 «О некоторых вопросах практики рассмотрения споров, связанных с заключением, исполнением и расторжением договоров банковского счета» // Хозяйство и право. 1999. № 9.

9. Постановление Пленума Верховного Суда РФ от 22.11.2016 № 54 «О некоторых вопросах применения общих положений Гражданского кодекса Российской Федерации об обязательствах и их исполнении» // Российская газета. 2016. 5 декабря.

10. Постановление Президиума ВАС РФ от 30.07.2013 № 1142/13 // Вестник ВАС РФ. 2014. № 1.

11. Белов В. А. Юридическая природа безналичных расчетов и «безналичных денег» // Бизнес и банки. 1998. № 52. С 4–5.

12. Ефимова Л. Г. Банковские сделки: право и практика. Москва: НИМП, 2001. 654 с.

13. Курбатов А. Я. Банковское право России: учебник для академического бакалавриата. 6-е изд., перераб. и доп. Москва: Юрайт, 2019. 349 с.

14. Степанова Д. И., Николаева Т. Е., Иволгина Н. В. Особенности организации и направления развития криптовалютных платежных систем // Финансы и кредит. 2016. № 10. С. 33–45.

15. Тарасенко О. А. Правовые проблемы исчисления сроков при осуществлении безналичных расчетов // Юридическая работа в кредитной организации. 2013. № 2 (36). С. 46–54.

16. Хрусталева А. В. Проблемы правового регулирования возврата платежа по спорной операции при безналичных расчетах в Российской Федерации // Закон. 2016. № 12. С. 58–69.

17. Чеклаукова Е. Л., Ермолина В. С. Анализ перспектив развития платежных систем в России // Сборник научных трудов Ангарского государственного технического университета. 2021. Т. 1, № 18. С. 329–335.

18. Шестопал О. Чем заменить SWIFT. Банковский рынок просчитывает последствия блокировки системы // Коммерсантъ. 2018. № 12.

Д. А. Топоров,
кандидат юридических наук, доцент,
Ростовский государственный экономический университет

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА РЕАЛИЗАЦИЮ ПРАВ СОБСТВЕННИКОВ ОБЪЕКТОВ НЕДВИЖИМОСТИ

Аннотация. Сегодня в РФ имеет место активное использование цифровых технологий в процессе регистрации в отношении объектов недвижимости, однако организован не чисто электронный документооборот, а смешанный бумажно-электронный способ закрепления права собственности и иных вещных прав в отношении недвижимого объекта. В настоящей статье анализируются особенности использования современных информационных технологий на гражданско-правовые отношения, складывающиеся в сфере рынка недвижимости. Изучаются различные аспекты процедуры государственной регистрации прав в отношении объ-

ектов недвижимости и заключения участниками рынка жилья электронных сделок в отношении недвижимого имущества, в том числе на примере сделок купли-продажи. Рассматриваются направления решения проблем правового обеспечения данной деятельности.

Ключевые слова: цифровизация, государственная регистрация недвижимости, сделка с недвижимым объектом, электронная форма сделки, электронная цифровая подпись (ЭЦП), электронный документ

THE IMPACT OF DIGITALIZATION ON THE REALIZATION OF HOUSING RIGHTS

Abstract. Today in the Russian Federation there is an active use of digital technologies in the registration process in relation to real estate objects, however, not a purely electronic document flow is organized, but a mixed paper-electronic method of securing property rights and other property rights in relation to an immovable object. This article analyzes the features of the use of modern information technologies on civil law relations developing in the real estate market. Various aspects of the procedure of state registration of rights in relation to real estate objects and the conclusion of electronic transactions in relation to real estate by participants of the housing market, including by the example of purchase and sale transactions, are studied. The directions of solving the problems of legal support of this activity are considered.

Keywords: Digitalization, State registration of real estate, Real estate transaction, Electronic form of transaction, Electronic signature, Electronic document

Введение. Право собственности на недвижимый объект с точки зрения его содержания заключается в наличии у собственника совокупности правовых возможностей по совершению в отношении него любых правомерных действий. Они могут быть ограничены законом или договором. Возникновение и реализация данных правомочий тесно связаны с институтом государственной регистрации прав в отношении объектов недвижимости. Полномочия изменяются при совершении тех или иных сделок в отношении недвижимого объекта.

Развитие цифровых технологий и их практическое использование носят массовый характер. Этот процесс породил ряд концептуальных юридических проблем, к примеру, обусловленных необходимостью определения допустимых пределов использования таких технологий и их возможного влияния на гражданские правоотношения, в том числе в сфере оборота объектов недвижимости. Цифровизация на государственном уровне признана одной из основных национальных целей развития [4].

Так, неслучайно Президентом Российской Федерации обозначена приоритетность принятия новых законов, которые требуются, по мнению главы государства, «для создания правовой среды новой, цифровой экономики, которые позволят заключать гражданские сделки и привлекать финансирование с использованием цифровых технологий, развивать электронную торговлю и сервисы» [5].

В условиях расширения практики использования современных цифровых технологий адекватной мерой стало изменение нормативного регулирования в рамках

Гражданского кодекса Российской Федерации (далее по тексту – ГК РФ [1]), в котором с 2019 г. нашли отражение возможности использования электронных ресурсов, в том числе электронных способов заключения сделок. Законодательные новеллы выступают ориентиром в процессе модернизации всего гражданского и гражданско-процессуального законодательства с учетом цифровой реальности. Нельзя не отметить, что, несмотря на отмеченную активность российского законодателя, правовая регламентация регистрации недвижимости имеет в настоящее время определенные пробелы, которые замедляют процесс развития рынка недвижимости в РФ.

В рамках изучения важнейших аспектов обозначенной тематики опубликован ряд научных работ, обобщающих теоретические и практические результаты использования цифровых технологий в оформлении гражданско-правовых отношений. Несмотря на это, представляется, что проблематика использования цифровых технологий применительно к рынку недвижимости освещена недостаточно, а представления о характере влияния цифровых технологий на частное право до сих пор носят дискуссионный характер. Сказанным обусловлена актуальность выбранной для рассмотрения темы.

Представляется целесообразным применительно к нормам гражданского и жилищного права рассмотреть особенности взаимовлияния цифровых технологий и частного права на примере оформления права на жилые помещения. Соответственно, цель работы заключается в формировании комплексного представления о влиянии цифровых технологий на оформление прав собственников жилых объектов.

В основу проведенного исследования положены метод сравнительного правоведения, логический метод, системный метод.

Результаты исследования состоят в формулировании выводов об особенностях правовой регламентации использования цифровых технологий при оформлении прав собственников недвижимых объектов на основе анализа нормативно-правовых актов, регулирующих данную сферу.

Проведен анализ результатов модернизации действующего гражданского законодательства и нововведения в сфере правового регулирования государственной регистрации в отношении объектов недвижимости и осуществления сделок с недвижимостью в условиях цифровизации и информатизации государства и общества.

Проведенное исследование привело к выводу, что имеющие место нововведения правового регулирования в сфере недвижимого имущества носят в целом позитивное значение, однако целесообразно устранение выявленных пробелов, что позволит улучшить качество нормативного обеспечения процесса модернизации общественных отношений в сфере оборота недвижимости.

Научная новизна проведенного исследования обусловлена самостоятельным анализом теоретических и практических аспектов использования цифровых технологий в отношении объектов недвижимости.

Практическая значимость исследования состоит в возможности использования полученных выводов в практической деятельности в сфере оформления прав в отношении жилья и других объектов недвижимости, использовать при заключе-

нии участниками рынка жилья электронных сделок в отношении принадлежащего им недвижимого имущества.

1. Современные подходы к использованию цифровых технологий в имущественной сфере. Цифровые технологии используются для совершения значимых с точки зрения права действий в отношении различных видов имущества, в том числе объектов недвижимости. Наблюдающееся взаимодействие феноменов цифровизации и постоянно модернизирующегося права обусловливает особенности их взаимного влияния.

Активное внесение изменений в один из основополагающих нормативных правовых актов (имеется в виду прежде всего упомянутый выше ГК РФ) путем включения норм, отражающих возможность использования электронных инструментов, стало закономерным ответом на складывающуюся правоприменительную практику. Такой подход законодателя призван снизить хаотичность в использовании цифровых технологий.

Сегодня перспектива роста автоматизации (технологизации, цифровизации) юридических процессов многими специалистами рассматривается как альтернатива традиционным правовым институтам. Как отметил коллектив авторов под руководством В. В. Зайцева, О. А. Серовой, «основные проблемы, определяющие негативные условия для трансформации правовой среды связаны с невозможностью эволюционного пути развития законодательства и права» [12. С. 28].

Использование цифровых технологий принято рассматривать как инструментальную основу реализации гражданских прав. Наблюдается диалектическое взаимодействие: современная цифровая форма реализации правоприменительной деятельности, радикально отличающаяся от формы, обусловленной включенностью в бумажный документооборот и требующей личных действий от участника отношений, не может не оказывать значимое воздействие на содержание данной деятельности; массовое и/или радикальное внедрение таких технологий меняет сущность не только отдельных институтов права, но и правовые принципы, топологию, саму суть правоприменительной деятельности.

Следует согласиться с В. А. Болдыревым, который справедливо отметил, что «построение отечественного законодательства о юридических лицах, правах на недвижимость, актах гражданского состояния базируется на дуалистическом подходе: фактические основания и материально-правовые последствия регистрации (содержание) разведены по разным законодательным актам с документами-основаниями и процедурами совершения регистрационных действий (формой) [7].

Итак, несмотря на предпринимаемые отечественным законодателем усилия, состояние регулирования посредством российского гражданского законодательства не отвечает потребностям участников рынка недвижимости.

2. Государственная регистрация объектов недвижимого имущества и сделок с ними с использованием электронных технологий. Сегодня представляется неоспоримым существенность активного влияния цифровых технологий на современное частное право и гражданский процесс. Осуществление процедуры государственной регистрации в отношении объектов недвижимости и совершение сделок с объектами недвижимости также испытывают данное влияние.

Недвижимые вещи, в том числе жилые помещения, при любом общественном устройстве рассматриваются как особо ценный имущественный объект, которому отводится особое место в системе общественных отношений. Это положение обусловлено той очевидной причиной, что с его функционированием связаны жизнь и деятельность людей во всех сферах экономики, управления и организации. Не в меньшей степени объекты недвижимости способствуют решению социальных вопросов, в частности, значимой для россиян жилищной проблемы.

Отдельной сферой широкого распространения цифровизации являются жилищная сфера и жилищное право. Жилищное право сегодня принято рассматривать как отрасль права, которая является неотъемлемой частью частного права. Предметом жилищного права выступают жилищные отношения (имеются в виду реально существующие общественные отношения), сопряженные с обеспечением прав граждан на жилье. Сегодня в жилищной сфере появилась возможность получения электронных государственных и муниципальных услуг посредством электронного общения, через электронные порталы [9].

Важность и значимость эффективного правового регулирования статуса недвижимости и динамики недвижимых объектов детерминирована тем обстоятельством, что данный вид имущества опосредует реализацию прав, гарантированных Конституцией Российской Федерации, а именно права на жилище и права на собственность. Данные конституционные права детализированы в важнейшем кодифицированном акте гражданского права – ГК РФ [1].

Нельзя не отметить, однако, что современное состояние правовой регламентации рассматриваемого правового института нельзя назвать в полной мере полным и удовлетворительным. Потенциально возможное расширение рынка недвижимости и ускорения оформления сделок с недвижимостью за счет использования цифровых технологий требует от юридической науки глубокого анализа проблем, с которыми сталкивается правоприменитель при заключении, исполнении договоров купли-продажи недвижимости, что позволит предложить научно обоснованные рекомендации по совершенствованию действующего законодательства.

Понятие недвижимости нашло легальное закрепление в п. 1 ст. 130 ГК РФ. Российский законодатель выделил ряд признаков, которые позволяют дифференцировать объекты недвижимости от иных, в том числе имеющих сходство с ними, имущественных объектов.

Ввиду особенностей объектов недвижимости законодатель закрепил в отношении них специальный правовой режим, который включает необходимость государственной регистрации. С 01.01.2017 наличие сведений о недвижимом объекте в Едином государственном реестре недвижимости (ЕГРН) выступает единственным легальным доказательством существования зарегистрированного права в отношении данного объекта.

На законодательном уровне предусмотрена возможность использования электронных технологий для регистрации прав в отношении объектов недвижимости. Так, в силу ст. 36.2 Федерального закона «О государственной регистрации недвижимости» закреплена возможность физического лица обратиться с заявлением, созданным в электронной форме, о внесении в ЕГРН соответствующей запи-

си о государственной регистрации таких фактов, как переход, прекращение права собственности в отношении недвижимого объекта. Законодатель распространил данную норму на любые недвижимые объекты, собственником которых является физическое лицо. Заявление такого рода подается с приложением необходимого пакета документов, которые подлежат удостоверению посредством использования усиленной ЭЦП [2]. Положения указанной статьи распространяются также в полной мере и на процедуру подачи заявлений о государственной регистрации договоров об уступке прав требований по договору участия в долевом строительстве.

Право на обращение в электронной форме может быть реализовано как непосредственно собственником жилья или иного недвижимого объекта, так и его законным представителем в силу закона либо его представителем, в этом случае полномочия последнего должны быть изложены в тексте доверенности, которая подлежит нотариальному удостоверению.

К подаваемому в электронной форме заявлению о государственной регистрации перехода, прекращения права собственности в отношении недвижимого объекта приобщается пакет документов, созданных в электронной форме, которые должны быть удостоверены усиленной квалифицированной электронной подписью заявителя. В ЕГРН с целью подтверждения данного факта вносится соответствующая запись. Собственник нескольких недвижимых объектов либо его представитель (в силу закона или нотариально удостоверенной доверенности) вправе подать заявление и пакет документов, подписанных посредством усиленной ЭЦП, как в отношении одновременно всех своих недвижимых объектов, право собственности на которые зарегистрировано в ЕГРН за собственником данной категории, так и в отношении каждого из них в отдельности.

Следует отметить, что российский законодатель не полностью отказался от бумажного документооборота в данной процедуре регистрации, т. е., как было отмечено выше, сконструировал электронно-бумажный способ взаимодействия Росреестра и гражданина. В силу п. 2 анализируемой статьи закона заявитель имеет обязанность предварительно в форме документа на бумажном носителе посредством личного обращения представить в Росреестр заявление о возможности регистрации права на принадлежащий ему объект недвижимости на основании документов, подписанных усиленной квалифицированной ЭЦП.

В силу п. 4 анализируемой статьи Федерального закона уже сам по себе факт отсутствия в ЕГРН такого заявления и внесенной на его основании записи о возможности регистрации права на недвижимый объект на основании заявления и пакета документов, подписанных посредством усиленной ЭЦП, закреплен в качестве основания для возврата поданного заявления о государственной регистрации и пакета приложенных к нему документов без рассмотрения, кроме прямо определенных законодательно случаев-исключений. Данное основание пресекает возможность регистрации права с использованием электронных технологий.

Обязанностью уполномоченного органа регистрации прав в отношении недвижимых объектов является уведомление собственника о факте подачи заявления, подтвержденного электронной подписью, в сроки и порядке, определенных нормативно.

Для реализации прав граждан самостоятельно посредством лишь электронных средств связи решить частноправовые проблемы потребуется материально-техническая база: установление в специально отведенных местах терминалов, считывающих оригиналы бумажно-печатных документов. Эти терминалы должны иметь прямой доступ к данным различных реестров, в том числе к реестру актов гражданского состояния и реестру брачных договоров, распечатывающих по желанию обратившихся лиц подтверждение совершения юридически значимого действия на бумажном носителе.

3. Использование цифровых технологий в сфере осуществления сделок с недвижимостью. Как показывают исследования, использование цифровых технологий при заключении сделок с недвижимостью постоянно возрастает, это тенденция как в России, так и в мировом масштабе [14. С. 601]. Проанализируем детально те возможности, которые открыты при использовании электронной цифровой подписи при совершении сделок с недвижимыми объектами.

Основная возможность состоит в том, что участники рынка недвижимости могут с ее помощью дистанционно оформить сделки купли-продажи или дарения недвижимости. Участники такого рода сделок могут физически находиться в разных концах страны и удостоверить свою личность, применив ЭЦП. Данная возможность крайне важна с учетом протяженности страны, а особенно актуальной она стала в период пандемии нового коронавируса и самоизоляции.

Рассматривая природу электронной цифровой подписи, следует отметить, что она является уникальным идентификатором личности, который присваивается конкретному физическому или юридическому лицу. Используются подписи, обладающие разной степенью защиты: в настоящее время выделяют простую и усиленную.

Электронная цифровая подпись с усиленной степенью защиты оформляется с целью, в частности, дистанционного участия в заключении сделок с объектами недвижимости, а также для получения возможности взаимодействия с порталами государственных органов и ведомств. Оформить усиленную ЭЦП следует заблаговременно в уполномоченных удостоверяющих центрах, аккредитованных в Минкомсвязи России.

Оформление усиленной ЭЦП представляет собой процедуру подтверждения подлинности личности, от имени которой подается виртуальный документ, что с юридической точки зрения позволяет приравнять его к бумажному аналогу.

Посредством использования электронной подписи уполномоченное лицо (собственник или его представитель) получает возможность дистанционно оформить сделку купли-продажи, дарения или мены объекта недвижимости. Также дистанционно подписываются договоры долевого участия и ипотечный договор. Процесс оформления необходимого пакета документов на объект включает сканирование документов, которые должны быть загружены на сайте Росреестра, при этом каждый участник сделки заверяет подаваемые электронные документы при помощи размещения ЭЦП, которая представляет собой файл в формате sig. Для осуществления такой процедуры используется специальное программное обеспечение – криптопровайдер. В отечественной практике наиболее широко применяется «КриптоПро CSP».

Позитивной стороной заключения сделок в отношении недвижимых объектов с использованием электронной цифровой подписи является высокая скорость регистрации. Также возникает возможность снижения издержек, поскольку при электронном оформлении размер госпошлины при их оформлении на сайте Росреестра сокращается на 30 %. Доступ к личному кабинету на сайте, помимо его владельца, имеют Росреестр, банк (при наличии ипотеки), а также девелопер [11].

Использование интернет-портала Росреестра с интуитивно понятным интерфейсом существенно упрощает получение рассматриваемого вида государственной услуги, в результате обслуживание граждан стало более качественным и доступным, значимо сократились его сроки. Также следует отметить, что органы нотариата с 01.01.2018 в свою очередь также осуществляют процедуру регистрации совершаемых нотариальных действий в электронном виде, в Единой информационной системе нотариата, в том числе данная процедура применима для оформления сделок с недвижимыми объектами. Как представляется, особенность рассматриваемого способа подачи документов заключается не только в высокой скорости рассмотрения заявления, но и удобном формате одного окна, при котором необходимый пакет собирает непосредственно нотариус, давая гарантию правильности составления документов и достоверности отраженных в них сведений.

Сегодня банки и девелоперы готовы предоставлять ипотечные кредиты и новостройки полностью бесконтактным способом [10].

Нельзя, однако, не отметить рост активизации мошенников при использовании дистанционных способов применительно к сделкам с недвижимыми объектами.

Востребованность цифровых сервисов, особенно позволяющих дистанционно осуществить регистрацию прав на недвижимые объекты, существенно возросла в период пандемии нового коронавируса.

В 2020 г., к примеру, была зафиксирована высокая активность использования электронных сервисов – как отмечается, имел место рост количества поданных электронных документов в сфере оформления ипотеки и регистрации договоров долевого участия в строительстве. Их совокупная доля от общего числа обращений в 2020 г. достигла 40 %. Указанный показатель выше данных предшествующего года в 1,5–2 раза [13].

В настоящее время активно проводится деятельность, направленная на консолидацию информационных систем федеральных органов исполнительной власти, аккумулирующих сведения о земле как основном объекте недвижимости. Она проводится в рамках эксперимента по созданию Единого информационного ресурса (ЕИР) об объектах в виде земельных участков и расположенной на них объектах недвижимости. В перспективе ЕИР позволит широкому кругу участников рынка в режиме онлайн получать полную и достоверную информацию об объектах недвижимости по принципу одного окна.

В 2019 г. государственная компания «Дом.рф», принадлежащая Правительству России в лице Агентства по управлению государственным имуществом. заявила о разработке и запуске сервиса для электронной регистрации сделок, проводимых с недвижимостью [8]. Этим сервисом при подписании документов по договорам

в отношении недвижимых объектов, обеспечивается юридическая гарантия как покупателю, так и продавцу. В дальнейшем представленный портал предполагается развивать в качестве единой цифровой платформы для всего рынка недвижимости страны.

27.06.2019 законодатель внес ряд изменений в Федеральный закон «Об участии в долевом строительстве многоквартирных домов и иных объектов недвижимости», которые закрепили возможность использования электронных ресурсов для застройщиков при заключении договоров участия в долевом строительстве [3].

Законодателем определено, что компетенция по установлению требований к договорам, соглашениям о внесении изменений в договор долевого участия, соглашениям об уступке прав требований по такому договору, совершаемым к электронной форме, принадлежит Росреестру как уполномоченному федеральному органу исполнительной власти, реализующему функционал в сфере нормативно-правового регулирования правоотношений, складывающихся при государственной регистрации прав в отношении недвижимого имущества и сделок с ним [6].

Близок к реализации проект создания в телекоммуникационной сети Интернет единого сервиса Росреестра в виде «виртуальной комнаты сделок» на доверенной цифровой платформе. Такой подход объединит всех участников оборота недвижимости и обеспечит необходимый уровень безопасности. Использование в данном сервисе возможностей искусственного интеллекта (ИИ) будет способствовать росту скорости и качества регистрации сделок с недвижимыми объектами. Отметим, что в случае успешной реализации данного проекта Росреестру удастся превзойти лучшие показатели сервисного обслуживания участников рынка недвижимости в мировом масштабе.

Реалии условий пандемии нового коронавируса и вынужденной самоизоляции в 2020–2021 гг. особенно заметно переориентировали и государственные органы, и частных лиц – участников сделок с недвижимостью с очного оформления сделок на использование дистанционных информационных технологий. Сегодня представляется неизбежным переход к усилению влияния цифровизации в сфере недвижимости. Многие компании осуществляют в этом направлении активную разработку и продвижение собственных продуктов и платформ. Особенность цифровизационного подхода заключается в отсутствии ограничений рынка недвижимости одной страной или территорией, в силу отсутствия физических границ для современных технологий.

В то же время в современных условиях быть полностью застрахованным от недобросовестности и мошеннических проявлений в виртуальном пространстве не может ни один из пользователей телекоммуникационной сети Интернет. Очевидная необходимость в дальнейшем расширении возможностей электронного документооборота в сфере заключения сделок в отношении недвижимых объектов порождает немало научных дискуссий как в отношении используемой терминологии, так и по вопросам практического правоприменения.

Проанализируем наиболее значимые пробелы правовой регламентации общественных отношений в сфере сделок с недвижимыми объектами:

– при чрезмерно высоком уровне угрозы утраты электронной информации и постороннего негативного вмешательства в содержание электронных докумен-

тов не разработан правовой механизм обеспечения их сохранности. Субъекты рынка недвижимости принципиально не готовы к тому, чтобы какая бы то ни было информация, созданная в виде электронного документа, будет сохранена только в сетевых ресурсах в отсутствие сохранения информации на бумажном носителе;

– созданная процедура подтверждения личности участников сделки в электронной форме не позволяет ни сотруднику регистрирующего органа, ни нотариусу убедиться в физическом и психическом состоянии участника сделки на момент ее оформления, достоверно оценить реальные, желаемые намерения. Участник виртуальной сделки, подтверждающий свою личность при помощи ЭЦП, потенциально может в этот момент находиться под негативным воздействием третьих лиц или утратить контроль над носителем, содержащим файл ЭЦП;

– полная доступность электронного документооборота всем россиянам на сегодняшний момент не обеспечена в силу особенностей информационного и коммуникационного развития России – как правило, отсутствует стабильный доступ к ресурсам телекоммуникационной сети Интернет в малонаселенных и труднодоступных местностях;

– удостоверяющие центры по выдаче ЭЦП не способны в полной мере обеспечить необходимый уровень информационной безопасности, это свидетельствует о необходимости в целях обеспечения безопасности сделок с недвижимостью дальнейшего совершенствования правового регулирования их деятельности.

Итак, проведенное исследование свидетельствует о необходимости нормативного закрепления единых стандартов и требований к электронным документам, обеспечению более высокого уровня информационной безопасности и защиты участников сделок на рынке недвижимости. Особенно важна защищенность физических лиц, продающих и покупающих жилые помещения.

В ближайшей перспективе необходимо нормативное закрепление дополнительных механизмов аутентификации участников сделок с недвижимыми объектами путем, в частности, идентификации личности граждан по лицу и голосу.

Заключение. Проведенное исследование показывает, что основной целью государственной регистрации сделок с недвижимым имуществом является полное приобретение права собственности или права пользования имуществом. Институт государственной регистрации сделок с недвижимым имуществом следует оценивать как фундаментальный институт, который гарантирует правомерность и легитимность заключаемой между субъектами правоотношений сделки, предусматривающей переход права собственности от одного субъекта к другому.

Основная значимость данного института состоит в обеспечении защиты прав участников рынка на принадлежащее им имущество, поддерживают стабильность и безопасность гражданско-правового оборота, упрощают систему налогообложения и т. п.

Гражданско-правовые сделки законодательно закреплены в качестве одного из юридических фактов, представляющих собой легитимные основания возникновения права на недвижимые объекты. Они представляют собой гражданско-правовые соглашения относительно прав на недвижимые объекты. Совершаемая сделка

признается действительной, когда она в полной мере соответствует установленным законом критериям.

Регистрация прав в отношении объектов недвижимости, вытекающих из сделок, производится в заявительном порядке на основании пакета документов, который с 2019 г. может предоставляться гражданами в уполномоченный орган в электронной форме, при этом процедура является электронно-бумажной.

Российским законодателем закреплен детализированный порядок предоставления государственной услуги по регистрации прав в отношении недвижимых объектов. Он предусматривает алгоритм действий как заявителя, так и органа, предоставляющего государственную услугу регистрации.

Исследование позволило выявить ряд пробелов законодательства в рассматриваемой сфере, которые могут быть устранены путем внесения соответствующих изменений в нормы гражданского законодательства РФ.

Выявленные недостатки и пробелы действующего законодательства РФ в рассматриваемой сфере, как представляется, целесообразно устранить путем издания единого нормативно-правового акта, в котором следует отразить все виды и признаки объектов недвижимости, обозначив критерии, на основании которых осуществляется выбор порядка осуществления государственной регистрации и отдельный алгоритм осуществления государственной регистрации в отношении определенных специальных объектов.

Подобный нормативный правовой акт позволил бы повысить эффективность правоприменительной деятельности при осуществлении государственной регистрации всех видов объектов недвижимости.

Список литературы

1. Гражданский кодекс Российской Федерации (часть 1) от 30.11.1994. № 51-ФЗ, принят ГД ФС РФ 21.10.1994 (с изм. и доп.) // СПС Консультант Плюс.

2. О государственной регистрации недвижимости: Федеральный закон от 13.07.2015 № 218-ФЗ (ред. от 14.07.2022) // Собрание законодательства Российской Федерации от 20.07.2015. № 29 (часть I). Ст. 4344.

3. О внесении изменений в Федеральный закон «Об участии в долевом строительстве многоквартирных домов и иных объектов недвижимости и о внесении изменений в некоторые законодательные акты Российской Федерации» и отдельные законодательные акты Российской Федерации: Федеральный закон № 151-ФЗ от 27.06.2019 (с изм. и доп.) // Собрание законодательства Российской Федерации от 1 июля 2019 г. № 26. Ст. 3317.

4. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента Российской Федерации от 07.05.2018 № 204 (с изм. и доп.) // Собрание законодательства Российской Федерации от 14.05.2018. № 20. Ст. 281.

5. Послание Президента Федеральному Собранию. 20.02.2019 // Официальный сайт Президента РФ. URL: http://www.kremlin.ru/events/president/news/59863

6. Балтутите И. В. Правовое регулирование оборота недвижимого имущества в условиях цифровизации российской экономики // Legal Concept = Правовая парадигма. 2021. Т. 20, № 1. С. 86–93. DOI: https://doi.Org/10.15688/lc.jvolsu.2021.1.13

7. Болдырев В. А. Система регистрационных действий // Законы России: опыт, анализ, практика. 2016. № 6. С. 79–86.

8. Запущен сервис для электронной регистрации сделок с недвижимостью – дом.рф. URL: https://www.xn – d1aqf.xn – p1ai/media/smi/zapushchen-servis-dlya-elektronnoy-registratsii-sdelok-s-nedvizhimostyu-dom-rf/

9. Калинин С. Ю. Гражданско-правовой режим недвижимости // Юридическая наука. 2015. № 3. С. 36.

10. Коннова Е. Электронная подпись в любых сделках с жильем. Что об этом надо знать // Жилье. 2020. 19 апр. URL:https://realty.rbc.ru/news/5e7dbd569a7947b68d61bbc1

11. Матыцин Д. Е., Балтутите И. В. Обеспечение исполнения государственных и муниципальных контрактов: банковские гарантии и цифровые технологии // Евразийский юридический журнал. 2020. № 11 (150). С. 133–136.

12. Цифровая экономика: проблемы правового регулирования / колл. авт.; отв. ред. В. В. Зайцев, О. А. Серова. Москва: КНОРУС, 2019. 200 с.

13. Росреестр планирует развивать цифровые платформы с учетом лучших международных практик. URL: https://rosreestr.gov.ru/press/archive/rosreestr-planiruet-razvivat-tsifrovye-platformy-s-uchetom-luchshikh-mezhdunarodnykh-praktik/

14. The model of distribution of human and machine labor at intellectual production in industry 4.0 / A. O. Inshakova, E. E. Frolova, E. P. Rusakova, S. I. Kovalev // Journal of Intellectual Capital. 2020. № 21 (4). Pp. 601–622.

Д. А. Черноусов,
аспирант,
Московский финансово-юридический университет,
мировой судья судебного участка № 242 Симоновского судебного района
г. Москвы

КОДЕКС ЭТИКИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА – ВЗГЛЯД НА САМОРЕГУЛИРОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ГРАЖДАНСКО-ПРАВОВЫХ ОТНОШЕНИЯХ

Аннотация. Статья посвящена исследованию Кодекса этики искусственного интеллекта (далее – ИИ) через призму гражданско-правовых отношений. Автор на основе анализа декларативного документа, позиций российских правоведов в области гражданского права выявляет характеристики рассматриваемого документа с точки зрения саморегулирования гражданско-правовых отношений в области искусственного интеллекта. Исследует обозначенные проблемы, подлежащие регулированию участниками-подписантами, выявленные в сравнении с текущей ситуацией в российском праве. Обращает внимание на предложенный термин акторов ИИ и его характеристики как один из признаков отнесения лица к возможности участия в добровольном использовании Кодекса. Делает вывод о влиянии рассматриваемого документа на гражданско-правовые отношения, необходимости учета его при исследованиях учеными, как обозначившего пробелы в праве непосред-

ственно технологическими компаниями, при разработке законодательства для регулирования ИИ в сфере цивилистических отношений.

Ключевые слова: гражданское право, искусственный интеллект, актор ИИ, право, саморегулирование, гражданско-правовые отношения, Кодекс этики искусственного интеллекта, национальная стратегия развития искусственного интеллекта

CODE OF ETHICS FOR ARTIFICIAL INTELLIGENCE – A VIEW ON SELF-REGULATION OF DIGITAL TECHNOLOGIES IN CIVIL LEGAL RELATIONS

Abstract. The article is devoted to the author's research on the Code of Ethics of Artificial Intelligence (hereinafter referred to as AI), through the prism of civil law relations. Based on the analysis of the declarative document, the positions of Russian lawyers in the field of civil law, the author reveals the characteristics of the document in question from the point of view of self-regulation of civil law relations in the field of artificial intelligence. Explores the identified issues to be regulated by signatory participants, identified in comparison with the current situation in Russian law. Draws attention to the proposed term of AI Actors and its characteristics as one of the signs that a person is eligible to participate in the voluntary use of the Code. He makes a conclusion about the impact of the document under consideration on civil law relations, the need to take it into account in research by scientists, as indicating gaps in law directly by technology companies, when developing legislation to regulate AI in the field of civil relations.

Keywords: Civil law, Artificial intelligence, AI actor, Law, Self-regulation, Civil law relations, Code of ethics for artificial intelligence, National strategy for the development of artificial intelligence

В мире ускоренными темпами растет использование в промышленности и в быту технологий с использованием искусственного интеллекта. Рост глобального рынка таких технологий, по расчетам экспертов [14, 15], в промежутке с 2022 по 2026 г. составит в среднем 18,6 % в год и достигнет 900 миллиардов долларов. Исследователи делят направления развития рынка по следующим категориям: услуги, программное обеспечение и аппаратное обеспечение. Рост рынка, в зависимости от категории, неравномерный, но в любом случае превышает 15 %, от его текущего объема в год. Что свидетельствует о высоком его уровне и необходимости пристального внимания как со стороны участников рынка, так и со стороны регуляторов. К ведущим странам в области развития технологий искусственного интеллекта на настоящий момент относят Китай, Россию, США, Японию, которые создали и опубликовали свои стратегии развития технологий искусственного интеллекта на среднесрочный период [16, 7, 17, 13], подразумевая, что данные технологии и их производные станут основой роста экономики и одной из точек для технологического превосходства. Что подталкивает к необходимости исследований в области права в части регулирования продуктов на основе технологии

искусственного интеллекта. Скорость изменения уровня технологий нарастает с каждым годом, что добавляет необходимости создания гибкой и приспосабливаемой системы подхода к регулированию отношений в области применения продуктов на основе технологии искусственного интеллекта в России. Исходя из приведенных данных, прогнозов исследователей рынков, наличия заинтересованности на государственном уровне в развитии технологий искусственного интеллекта в ведущих странах мира, тема исследования представляется автору актуальной.

В России регулирование на правовом уровне данных технологий представлено: Федеральным законом от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"»; Указом Президента РФ от 10.10.2019 № 490, «О развитии искусственного интеллекта в Российской Федерации» (далее Указ Президента РФ) (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года» – далее Стратегия) [7]; Распоряжением Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» (далее – Распоряжение Правительства РФ) [19]. Кроме того, разработан ряд ГОСТов для применения технологии ИИ в различных направлениях, а также для оценки качества систем на основе технологий искусственного интеллекта. В конце октября 2021 г. некоторыми из российских технологических компаний был создан и согласован Кодекс этики в сфере ИИ, который направлен на применение систем на основе технологии ИИ в гражданской сфере.

Существующие проблемы в области правового регулирования систем на основе искусственного интеллекта и их применения в России частично обозначены распоряжением Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» [19. С. 4]. К ним, например, отнесены: соблюдение баланса между требованиями по защите персональных данных и необходимостью их использования для обучения систем искусственного интеллекта; определение предмета и границ регулирования сферы использования систем искусственного интеллекта и робототехники; ответственность за причинение вреда с использованием систем искусственного интеллекта и робототехники; правовой режим результатов интеллектуальной деятельности, созданных с использованием систем искусственного интеллекта. Как указано в Национальной стратегии развития искусственного интеллекта России [7. С. 2], необходимо адаптировать в нормативно-правовом отношении в части взаимодействия человека и систем на основе технологий искусственного интеллекта, выработать этические нормы применения ИИ. Также определен срок приведения нормативно-правовой базы к условиям стремительных изменений в области технологий искусственного интеллекта для своевременного и безопасного регулирования таких систем с обязательным стимулированием развития техноло-

гий искусственного интеллекта. Как видится автору из Стратегии развития правового регулирования ИИ в России, ему отдается не последнее место в условиях развития новой отрасли. Поиск баланса между необходимостью регулирования и уровнем свободы отрасли от лишних бюрократических факторов непосредственно влияет на скорость развития систем на основе искусственного интеллекта, а также дает синергетический эффект при правильном его подборе для развития страны. С учетом необходимости соблюдения прав человека, сохранности персональных данных, безопасности людей и подконтрольности систем на основе искусственного интеллекта автор делает вывод о наличии изначально требуемых существенных ограничений и необходимости чуткого подхода к регулированию области применения таких систем для недопущения перерегулированности и снижения тормозящего действия правовых норм. На настоящий момент основными вопросами для исследований в области правового регулирования систем искусственного интеллекта автор считает исследование всех видов ответственности при использовании систем с искусственным интеллектом во всех областях гражданского общества. При этом стоит отметить, что саморегулирование в данном вопросе уже представлено в России.

Так, 26.10.2021 [18] на I Международном форуме «Этика искусственного интеллекта (ИИ): начало доверия» подписан «Кодекс этики искусственного интеллекта» (далее – Кодекс) [12]. Данное действие положило начало добровольному регулированию проблем, связанных с этикой искусственного интеллекта, ограничением использования искусственного интеллекта, а также концепции ответственности за результаты деятельности систем ИИ, которую поддержало технологическое сообщество.

Кодекс имеет рекомендательный характер для всех присоединившихся лиц [12. С. 9], однако в свете добровольного присоединения и, по сути, отсутствия репрессивного аппарата, по мнению автора, будет более приемлем на первоначальном этапе регулирования гражданских правоотношений, чем государственное регулирование.

На момент написания статьи в число участников – подписантов Кодекса включено 100 крупных технологических компаний России, включая все крупные телекоммуникационные компании и ведущие университеты.

Сам Кодекс состоит из преамбулы и двух разделов. Первый раздел касается принципов этики и правил поведения подписантов при осуществлении ими разработки, внедрения, использования и предоставления услуг, связанных с ИИ. Второй отдельно оговаривает порядок использования Кодекса. По мнению автора, стоит начать рассмотрение Кодекса со второй части.

Отдельно оговорено, что весь Кодекс базируется на законодательстве России, начиная с Конституции РФ и международных договоров ратифицированных и действующих для Российской Федерации и заканчивая стратегиями развития ИИ [12. С. 8]. Что говорит о глубокой проработке принципов Кодекса и учете возможных пробелов права, замеченных его создателями, не урегулированных прямо законодательством РФ. Отдельно в тексте дано только понятие акторов ИИ [12. С. 8] и перечислены относящиеся к ним лица, по критериям. По набору признаков, относящих лицо к акто-

ру ИИ, можно сделать вывод о самом широком круге из возможных, который авторы постарались внести в возможные подписанты Кодекса. Поскольку к ним отнесены как разработчики и программисты, так пользователи и получатели услуг на основе систем искусственного интеллекта (далее – СИИ). Остальные же термины применимые в рамках рассматриваемого документа предлагается брать из действующего законодательства и использовать в установленном законом виде и порядке.

При этом, несмотря на наличие во второй части раздела, посвященного механизму присоединения и реализации Кодекса, четко установленных правил порядка реализации его не описано [12. С. 9–10]. Положениями предполагается создание Комиссии по реализации Национального кодекса в сфере этики ИИ на базе Ассоциации «Альянс в сфере искусственного интеллекта», при участии иных заинтересованных организаций [12. С. 10]. Полномочия комиссии, документы, ей издаваемые, обязательность решений комиссии для участников, возможность оспаривания, порядок разрешения споров и т. п. не установлены.

Первый раздел Кодекса разделен на шесть параграфов, которые устанавливают основные принципы и правила проектирования ИИ, использования его и применения в гражданском обороте.

Первый из них устанавливает следующие принципы развития технологий ИИ: Человеко-ориентированный и гуманистический подход; Уважение автономии и свободы воли человека; Законность; Отсутствие дискриминации; Оценка рисков и гуманитарного воздействия [12. С. 1–3]. По мнению автора, данный набор принципов, имея декларативный характер, говорит о том, что подход разработчиков Кодекса обстоятелен, имеет долгосрочную ориентацию в правовом поле, в том числе и нацеленность на регулирование принципиальных моментов технологий, которые могут оказывать воздействие на общество в целом.

Второй параграф направлен на установление ответственного отношения акторов ИИ к разработке и использованию таких систем. Декларирует принципы взаимодействия человека с ИИ, находящимся в гражданском обороте, и устанавливает принципы проектирования таких отношений, проектирования безопасности систем искусственного интеллекта и базовые принципы, применимые в гражданском обороте, по мнению создателей Кодекса [12. С. 3–5]. Также данный параграф в своем последнем пункте устанавливает необходимость контроля совершенствования ИИ для выявления предпосылок формирования «сильного ИИ», который на настоящий момент воспринимается футурологами как возможная существенная опасность [1. С. 106]. Проведенный автором анализ второго параграфа подтверждает первоначальную мысль о саморегулировании крупными участниками гражданского оборота на настоящий момент гражданско-правовых отношений в свете наличия пробельности законодательства и в свете плотной работы в данном направлении – декларированию предпосылок для выделения отдельной области права, которая будет регулировать отношения, связанные с ИИ в долгосрочной перспективе.

Создавая данный Кодекс, по мнению автора, участники реализации инициативы правильно выделили в третьем параграфе первой части основную мысль, касающуюся ответственности лиц, занимающихся разработкой, использованием и применением технологий ИИ в гражданско-правовом обороте, – ответствен-

ность за действия ИИ несет человек. Несмотря на непроработанность данного утверждения с точки зрения права, отсутствия аргументации и объема, уделенного данному вопросу. Мысль об ответственности человека за действия ИИ – на текущий момент основная в юридическом поле. Вне зависимости от того, кто является конечным ответственным лицом, – пользователь или разработчик, физическое или юридическое лицо или иные лица.

Четвертый параграф закрепляет прикладной характер использования технологий ИИ для наибольшей пользы, в соответствии с назначением, заявляемым при разработке, и развитие устанавливаемого Кодексом подхода для всех разработчиков при внедрении и проектировании систем ИИ [12. С. 6]. Анализируя данные принципы, стоит отметить, что они вписываются в стратегию саморегулирования и заложения основ гражданско-правового регулирования в отношении ИИ в части, не урегулированной правом, и, возможно, являются первым шагом к выделению области права, как предполагалось ранее.

Пятый параграф, устанавливает частичный отказ от конкуренции и обмен опытом в развитии технологии ИИ для совместного повышения уровня компетентности участников [12. С. 6–7]. Что вполне согласуется с «Национальной стратегией развития искусственного интеллекта», утвержденной Указом Президента РФ, и выработанным на ее основе распоряжением Правительства РФ.

Шестой параграф констатирует необходимость поднятий уровня доверия к технологиям на базе ИИ, используемым в гражданском обороте путем открытости и добросовестности акторов ИИ и определенности их действий на базе выработанных этических принципов [12. С. 7–8].

Суммируя анализ Кодекса, с точки зрения автора, можно установить нижеследующие закономерности. Данный документ, подписанный и принятый к исполнению ведущими участниками рынка технологий ИИ в нашей стране, является саморегулирующим документом в области гражданско-правовых отношений, в части, не урегулированной правом. Попыткой выделить в отдельную область права правоотношения человека и ИИ, в которой необходимо установить основные принципы работы на базе Стратегии, утвержденной Указом Президента РФ по развитию таких технологий. Несмотря на наличие критики в адрес Стратегии и необходимости дальнейших исследований правоведов [3. С. 53]. Стоит отметить, что рассматриваемый документ, в отличие от иных стран, озаботившихся регулированием области этики в гражданско-правовых отношениях при использовании технологий ИИ, принят не государственным органом, а как инициатива ведущих компаний и разработчиков.

Подводя итоги исследования появления данного документа, его влияния на гражданско-правовые отношения в государстве, хотелось бы выделить основные моменты. Первоначальная инициатива негосударственных объединений в области регулирования и установления правил для использования систем искусственного интеллекта в гражданско-правовых отношениях показывает не только злободневность вопроса, но и назревший вопрос устранения пробелов законодательства [8. С. 22–23] хотя бы в таком декларативном виде, для добровольного присоединения. Сигнал государству был подан со стороны значимых в экономическом плане

лиц, которые ответственно подошли к вопросу обозначения принципов и норм как этики, так и стратегии развития технологии ИИ в стране, полностью понимая свою ответственность и необходимость следовать государственным интересам. Альянс в сфере искусственного интеллекта поднял в том числе и вопрос ответственности за действия ИИ, который на настоящий момент предлагает решать в соответствии с имеющимся законодательством, как понятно в любой области, в том числе и в рамках гражданско-правовых отношений. При этом ответственность за действия ИИ предлагается возлагать на юридическое или физическое лицо, в соответствии с мерой ответственности за принятия решения о выполнении тех или иных действий, которые полагается фиксировать в рамках управления системами ИИ, поскольку это обязанность субъекта права – соблюдать требования, установленные юридической нормой [10. С. 8; 6. С. 182]. Как бы в дальнейшем ни решался вопрос об искусственном интеллекте и его месте в гражданско-правовых отношениях, выделении его в отдельное направление права, оставление его существующим объектом права, наделением его частично правосубъектностью [11. С. 2–3; 2. С. 236–238; 5. С. 35–42], нельзя не признать, что ответственность в системах с технологиями ИИ на настоящий момент могут нести только юридические и физические лица ввиду отсутствия «сильного ИИ» и только поиска предпосылок к возможности его возникновения. В части установления приоритета прав человека при общении с СИИ и иных принципов, которые были описаны ранее, автор предлагает при формировании нормативно-правовой базы обязательно учесть положения, взятые за принципы организации гражданско-правовых отношений, выработанные в порядке саморегулирования технологическими компаниями России для соблюдения законодательства и дополнить их в соответствии с разработками ученых-правоведов [12, 225; 9. С. 17–19] в части исследования систем ИИ с точки зрения гражданско-правовых отношений – использовать в государственном регулировании цивилистических отношений.

Список литературы

1. Бостром Н., Искусственный интеллект. Этапы. Угрозы. Стратегии / пер. с англ. С. Филина. Москва: Манн, Иванов и Фербер, 2016.

2. Габов А. В., Хаванова И. А. Эволюция роботов и право XXI века // Вестник Томского государственного университета. 2018. № 435. С. 220–238.

3. Каплиев А. С. Критика национальной стратегии развития искусственного интеллекта на период до 2030 года // Право и государство: теория и практика. 2020. № 2 (182). С. 51–53.

4. Котлярова В. В. Права искусственного интеллекта // Дневник науки. 2019. № 51. URL: http://dnevniknauki.ru/images/publications/2019/5/philosophy/Kotlyarova_Shemyakina.pdf (дата обращения: 19.09.2022).

5. Морхат П. М. Юнит искусственного интеллекта как электронное лицо // Вестник Московского государственного областного университета. 2018. № 2.

6. Овчинникова Т. А. Понятие и структура института юридической ответственности // Образование и право. 2022. № 2. С. 180–182.

7. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 г.» от 10.10.2019. № 490 // Собрание законодательства Российской Федерации. 14.10.2019. № 41. Ст. 5700.

8. Федотов М. А. Киберпространство как сфера обитания права // Бюллетень ЮНЕСКО по авторскому праву. 1999. Т. XXXII, № 1. С. 21–30.

9. Федотов М. А. Роль университетской науки в формировании права искусственного интеллекта // Цифровая среда и политика университетов в сфере интеллектуальной собственности: сб. научных работ / отв. ред. проф. И. А. Близнец. Москва: Издательская группа «Юрист», 2021. С. 9–19.

10. Юзефович Ж. Ю. Функции юридической ответственности и формы их реализации по российскому законодательству: специальность 12.00.01 «Теория и история права и государства; история учений о праве и государстве»: дис. … канд. юрид. наук. Москва, 2004. 172 с.

11. Ястребов О. А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права РАН. 2018. № 2. URL: https://cyberleninka.ru/article/n/pravosubektnost-elektronnogo-litsa-teoretiko-metodologicheskie-podhody (дата обращения: 18.09.2022).

12. Кодекс этики в сфере искусственного интеллекта. URL: https://a-ai.ru/wp-content/uploads/2021/10/Кодекс_этики_в_сфере_ИИ_финальный.pdf (дата обращения: 18.09.2022).

13. URL: https://www8.cao.go.jp/cstp/ai/aistratagy2019.pdf (дата обращения: 18.09.2022).

14. URL: https://www.cnews.ru/reviews/ii_2022/articles/vyruchka_krupnejshih_postavshchikov_ii (дата обращения: 18.09.2022).

15. URL:https://ict.moscow/research/mirovoi-rynok-iskusstvennogo-intellekta-2021–2028/ (дата обращения: 18.09.2022).

16. URL: http://www.gov.cn/zhengce/content/2017–07/20/content_5211996.htm(дата обращения: 18.09.2022).

17. URL: https://www.govinfo.gov/content/pkg/FR-2019–02–14/pdf/2019–02544.pdf (дата обращения: 18.09.2022).

18. URL: https://rg.ru/2021/10/26/v-rossii-podpisan-kodeks-etiki-iskusstvennogo-intellekta.html (дата обращения: 18.09.2022).

19. Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства РФ. 31.08.2020. № 35. Ст. 5593.

Л. В. Шварц,
кандидат юридических наук, доцент
И. С. Белобородов,
магистрант,
Северо-Западный институт управления
Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации

КРАУДФАНДИНГ: ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ТЕРМИНОЛОГИИ, ЗАКОНОДАТЕЛЬСТВА И ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ

Аннотация. Цель исследования: провести анализ положительных и отрицательных положений законодательства об инвестировании с помощью цифровых платформ. В статье изучена проблема определения правовой природы краудфандинга, рассмотрен правовой статус участников крауд-отношений. Результаты исследования: предложены авторские рекомендации относительно требуемых изменений в действующее законодательство в целях полноценного правового регулирования данного финансового инструмента. В итоге авторы пришли к следующим выводам: требует доработки механизм по раскрытию и предоставлению информации на краудфандинговых площадках, необходимо ввести налоговые льготы как стимулирующий фактор развития краудфандинга, представляется возможным разрешить иностранным компаниям участвовать в крауд-отношениях в России как лицам, привлекающим инвестиции.

Ключевые слова: право, законодательство, цифровая экономика, краудфандинг, инвестирование, финансирование проектов, инвестиционная платформа, инвестор, оператор инвестиционной платформы, лицо, привлекающее инвестиции

CROWDFUNDING: SEPARATE PROBLEMS OF TERMINOLOGY, LEGISLATION AND LAW ENFORCEMENT PRACTICE

Abstract. The purpose of the study: to analyze the positive and negative provisions of the legislation on investing using digital platforms. The article examines the problem of determining the legal nature of crowdfunding, examines the legal status of participants in crowd relations. Research results: the author's recommendations on the required changes to the current legislation in order to fully regulate the legal regulation of this financial instrument are proposed. As a result, the authors came to the following conclusions: the mechanism for disclosure and provision of information on crowdfunding platforms needs to be improved, tax incentives should be introduced as a stimulating factor in the development of crowdfunding, it is possible to allow foreign companies to participate in crowd relations in Russia as individuals attracting investments.

Keywords: Law, Legislation, Digital economy, Crowdfunding, Investment, project financing, Investment platform, Investor, Investment platform operator, Person attracting investments

В современном мире появляются и становятся востребованными новые способы увеличения имущественного капитала. Причиной этому выступает посте-

пенная цифровизация всех сфер общества, в том числе и экономической, в связи с чем государство должно своевременно создавать нормативно-правовое поле для недавно появившихся инструментов привлечения денежных средств, одним из которых является краудфандинг.

По поручению Президента РФ была разработана Стратегия развития малого и среднего предпринимательства в РФ на период до 2030 г. (распоряжение Правительства РФ от 2 июня 2016 г. № 1083-р), в которой предлагалось развивать новые источники финансирования проектов для малых и средних предприятий.

В рамках реализации этого документа стратегического планирования с 1 января 2020 г. вступил в силу Федеральный закон № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Закон о краудфандинге).

Принимая этот закон, законодатель преследовал определенные цели, а именно:

– нормативно закрепить краудфандинг на законодательном уровне, т. е. создать отдельно правовую базу, регулирующую данный механизм привлечения денежных средств и устранить правовую яму в отношении деятельности российских краудфандинговых платформ;

– защитить стороны данных правоотношений, в особенности инвесторов;

– закрепить новую возможность привлечения инвестиций для малого и среднего бизнеса как альтернативного инструмента финансовой поддержки.

Данные цели достигаются путем создания определенных условий, в которых этот механизм будет адекватно реализовываться.

Обратимся, прежде всего, к анализу интересующего нас понятия. В данном законе, хотя его и принято именовать Законом о краудфандинге, в названии и в тексте закона термин «краудфандинг» не употребляется, так как его было решено убрать и заменить на «инвестирование и привлечение инвестиций с использованием инвестиционных платформ». Даже при беглом ознакомлении с содержанием закона становится ясно, что законодатель урегулировал только краудинвестинг и краудлендинг, т. е. такие модели инвестирования, целью которых является получение определенной прибыли от вложений. Между тем изначально понятие краудфандинга не включало в себя инвестирование как таковое, здесь больше подходило словосочетание «возможность поддержать» на безвозмездной основе или получить взамен какой-нибудь небольшой подарок [4. С. 210]. Получается, на благотворительные и условно-возвратные модели, где участник компании может поддержать проект безвозмездно или получить нефинансовое вознаграждение, не распространяется действие данного акта, поэтому они остаются вне специального урегулирования, а участникам приходится руководствоваться общими нормами гражданского и налогового законодательства. Однако термином «краудфандинг» в современном языковом употреблении принято обозначать добровольное совместное финансирование какого-либо проекта или организации, а платформы действуют как посредники для привлечения этого капитала. Поэтому понятие краудфандинга понимают многосторонне и многоаспектно вследствие широты самого явления.

Возникает закономерный вопрос: если законодательное закрепление краудфандинга появилось только со вступлением в силу данного Закона о краудфандинге 2020 г., тогда на какой нормативно-правовой базе функционировали краудфандинговые площадки ранее? Впервые на высоком государственном уровне в России заговорили о будущем народного финансирования – краудфандинга – 17 декабря 2014 г. на заседании нижней палаты в рамках обсуждения повышения уровня инвестиционной активности в социальные и инновационные проекты и необходимости законодательных инициатив в этой сфере [8. С. 191]. Результатом стали рекомендации о внесении изменений в Налоговый кодекс РФ, формировании инструмента государственно-частного партнерства и т. п.

Как следствие, было опубликовано Письмо ФНС России от 25 ноября 2016 г. № СД-4–3/22415@ «О налогообложении средств, полученных посредством краудфандинга», в котором говорилось о налоге на прибыль при безвозмездном получении имущества (денежных средств) посредством краудфандинга. К слову сказать, содержащийся в этом налоговом документе термин «краудфандинг» был взят из Википедии, исходя из которой это сотрудничество людей, добровольно объединяющих свои ресурсы, как правило, через сеть Интернет, чтобы поддержать усилия других.

Следующим правовым этапом формирования и развития краудфандинга стало вышеупомянутое распоряжение Правительства РФ от 2 июня 2016 № 1083-р, где указывалось, что в рамках реализации Стратегии будут предложены решения для развития краудфандинга и краудинвестинга для целей поддержки малого и среднего бизнеса.

Немалую роль в разработке концепции регулирования краудфандинга сыграл Банк России. С 2015 г. ЦБ РФ проводит мониторинг краудфандинговых площадок, разрабатывает планы мероприятий (дорожные карты) регулирования рынка краудфандинга в соответствии с основными направлениями развития финансового рынка Российской Федерации [1. С. 540]. При этом Банк России определяет краудфандинг как механизм привлечения заемных средств либо коллективного финансирования компаний или проектов с использованием интернет-площадок [6].

Краудфандинг как финансовый механизм поддержки малого и среднего бизнеса нашел свое закрепление и в опубликованных в 2018 г. Методических рекомендациях органам исполнительной власти субъектов Российской Федерации и органам местного самоуправления, способствующих увеличению доходной базы бюджетов субъектов Российской Федерации и муниципальных образований, где обозначены плюсы краудфандинга по сравнению с традиционными формами инвестиций, а именно: связь с конечным потребителем продукта, отсутствие профессионального посредника и возможность вложения небольших по размеру вкладов, что более привлекательно для большого числа людей; притом что существует риск, связанный с новизной данного механизма и ограниченностью доступа инвестора к информации.

Завершающим этапом стало внесение на рассмотрение Государственной Думой в 2018 г. законопроекта № 419090–7 с первоначальным названием «Об альтернативных способах привлечения инвестиций (краудфандинге)», где под краудфандингом понималась деятельность по организации розничного финанси-

рования. Разработчики предлагали использовать в качестве современной формы краудфандинга приобретение токенов инвестиционного проекта, а также использовать смарт-контракты. При этом определение «токенов» и «смарт-контракта» предполагалось дать в отдельном федеральном законе, регулирующем отношения, связанные с цифровым (виртуальным) имуществом. Однако текст законопроекта, принятого в первом чтении, существенно отличается от первоначально представленного варианта. В нем уже не фигурирует термин «краудфандинг», а вместо него вводится понятие «деятельность по организации привлечения инвестиций» и, как следствие, название законопроекта тоже изменилось. Стоит ли говорить, что на выходе мы получили совершенно иной закон, существенно отличающийся от первичного варианта, регулирующий не только краудфандинг, но и другую условно инвестиционную деятельность.

Инвестором на платформе может выступать любое физическое или юридическое лицо, поэтому Законом о краудфандинге предусмотрены определенные меры по защите их прав, как наиболее уязвимой стороны в краудфандинговых отношениях, что в целом соответствует мировой практике. Так, к основным элементам механизма минимизации рисков инвесторов можно отнести:

– требование к оператору инвестиционной платформы информировать инвестора о всех участниках краудфандинга и публиковать всю необходимую информацию, установленную Законом о краудфандинге;

– ограничение суммы инвестиционных вложений для физических лиц до 600 тысяч рублей;

– обязанность оператора убедиться в том, что инвестор понимает все риски и возможность потери всех своих инвестиций;

– полный возврат денежных средств оператором инвестиционной платформы инвестору, если не был достигнут минимальный размер необходимых средств;

– возможность отказа инвестора от инвестиционного предложения в течение пяти рабочих дней со дня, когда он принял данное предложение, но не позднее дня, когда оно прекратится.

При этом остаются вопросы, требующие разрешения. Так, обязанность оператора инвестиционной платформы о необходимости информирования инвестора о том, что инвестиционная деятельность является высокорисковой и он может полностью потерять все вложенные средства, относится только к инвесторам – физическим лицам (на это прямо указано в ч. 7 ст. 3 Закона о краудфандинге), что является спорным моментом, так как инвестор – юридическое лицо также может не осознавать все риски, поэтому представляется, что данная обязанность должна распространяться на всех участников краудфандинговых правоотношений.

Другим значимым моментом является тот факт, что инвестор подтверждает свое ознакомление со всей информацией путем принятия правил инвестиционной площадки нажатием «Кнопки» (например, в п. 1 Правил инвестиционной платформы Jetlend), что означает полное согласие лица (инвестора и лица, привлекающего инвестиции) с правилами инвестиционной платформы. Законодателем определено, что такое заверение должно быть обязательно перед использованием платформы, однако им не установлено, в какой именно форме такое заверение должно происходить, поэтому каждая платформа выбирает свой вариант такого

согласия, в том числе и путем нажатия «Кнопки». Справедливости ради заметим, что на многих зарубежных краудфандинговых платформах заверение происходит таким же способом. Однако данное решение является неоднозначным: с одной стороны, так упрощается процедура для всех сторон данных отношений, но с другой – такое заверение нельзя назвать надежным подтверждением всех рисков, которые может понести инвестор. Представляется необходимым сформировать более надежный, но при этом не усложняющий краудфандинговые отношения механизм подтверждения информированности инвестора.

На наш взгляд, для того, чтобы краудфандинг был более привлекателен и продуктивен, имеет место введение налогового вычета для инвестиций, привлеченных на краудфандинговых площадках, по аналогии с инвестиционным счетом (ст. 219.1 НК РФ). Такая возможность предусмотрена в некоторых зарубежных странах, например, в Великобритании (30 %), что привело к большей востребованности платформ.

К оператору инвестиционной платформы как участнику рассматриваемых отношений предъявляются определенные требования (к его статусу и организационной форме). Оператором инвестиционной платформы является хозяйственное общество, осуществляющее деятельность по организации привлечения инвестиций и включенное Банком России в реестр операторов инвестиционных платформ. В соответствии со ст. 76.1 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» оператор инвестиционной платформы является некредитной финансовой организацией. Это связано с тем, что в соответствии с Законом о краудфандинге оператор инвестиционной платформы получает денежные средства инвесторов на свой номинальный счет, далее передает лицу, привлекающему инвестиции либо возвращает инвесторам.

Однако если проводить анализ отнесения оператора инвестиционной платформы к некредитным финансовым организациям, то можно увидеть, что есть определенная недоработанность в законодательстве, а именно в п. 2 ст. 180 Федерального закона от 26 октября 2002 г. № 127-ФЗ «О несостоятельности (банкротстве)» и п. 6 ст. 4 Федерального закона от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции», где речь идет о финансовых организациях, оператора инвестиционной платформы среди них нет.

Оператор цифровых платформ имеет право совмещать свою деятельность с другой финансовой деятельностью, предусмотренной п. 2 ст. 10 Закона о краудфандинге. Данный перечень не является исчерпывающим, но с условием возможности такого совмещения, предусмотренного законодательством, однако неясно, вправе ли оператор инвестиционной платформы заниматься нефинансовой деятельностью [2. С. 28–29]. Считаем, что в законе следовало бы прописать исключительную деятельность оператора инвестиционной платформы.

Помимо этого, оператор инвестиционной платформы должен иметь капитал в размере 5 млн рублей. Здесь явно прослеживается аналогия формирования капитала организаторов торгов. Также закон содержит требование о соответствии лиц, имеющих право прямо или косвенно (через подконтрольных ему лиц), самостоятельно или совместно с иными лицами, связанными с ним договорами, распоряжаться 10 % и более голосов, приходящихся на голосующие акции/доли, состав-

ляющие уставный капитал оператора инвестиционной платформы, а также членов органов управления требованиям Закона о краудфандинге [3. С. 7].

В завершение оператор инвестиционной платформы должен быть включен в Реестр в соответствии со ст. 17 Закона о краудфандинге и Указания Банка России от 4 декабря 2019 г. № 5342-У «О порядке ведения реестра операторов инвестиционных платформ». Банк России проверяет достоверность предоставленных оператором данных, соответствие требованиям, после чего принимает решение о включении в реестр, тем самым легализуя его деятельность [7].

Для полноценного осуществления механизма краудфандинга необходим еще один субъект – это лицо, привлекающее инвестиции. Законом о краудфандинге, а именно в пп. 5 п. 1 ст. 2, указано, что лицом, привлекающим инвестиции, признается юридическое лицо или индивидуальный предприниматель, которым оператор инвестиционной платформы оказывает услуги по привлечению инвестиций. При этом к такому лицу предъявляются общие требования, которые прописаны в ст. 14 Закона о краудфандинге: отсутствие сведений о причастности к экстремистской или террористической деятельности; а также соответствие правилам, действующим на конкретной цифровой платформе.

Стоит обратить внимание, что в данной статье содержится уточнение по требованиям, предъявляемым к юридическим лицам и индивидуальным предпринимателям, в частности различие в банкротных делах. Разница между условиями ограничения использования инвестиционной платформы зависит от этапа банкротства: в отношении юридического лица дело о банкротстве должно быть возбуждено, а в отношении индивидуального предпринимателя введена процедура банкротства.

Что касается максимальной суммы, которую могут привлечь вышеупомянутые лица, она равняется 1 миллиарду рублей за один календарный год, при этом составление и регистрация проспекта ценных бумаг не обязательны, что является таким же требованием, как и к эмитенту, который размещает эмиссионные ценные бумаги, в соответствии с пп. 4 п. 1 ст. 22 Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг». Данное ограничение является обычной практикой законодателя стран, где краудфандинг нормативно закреплен, при этом контроль за максимально допустимой суммой возложен на оператора инвестиционных платформ, что является закономерным действием.

Заметим, что на отдельных инвестиционных платформах могут устанавливаться дополнительные требования к лицам, привлекающим инвестиции. Так, например, в правилах платформы Fair finance установлено, что у заемщика не должно быть задолженности перед налоговой службой более пяти тысяч рублей, а сумма ежемесячных оборотов за последние восемь месяцев составляет не менее ста тысяч рублей. Конкретно к юридическим лицам предъявляются следующие дополнительные требования: с даты регистрации лица прошло более 10 месяцев и адрес регистрации не является адресом массовой регистрации [5].

Также необходимо отметить, что, хоть законодателем и указан перечень необходимых требований и условий для лица, привлекающего инвестиции, однако инвестор несет риск асимметрии информации (т. е. инвестор владеет информацией, которая была предоставлена информационной платформой, и у него отсут-

ствует как таковая возможность проверки информации на уровне проекта), поэтому представляется целесообразным проверять хозяйственную деятельность лица, привлекающего инвестиции, как до, так и после начала деятельности на инвестиционной площадке, в том числе проводить юридическую проверку проекта и базовую проверку бизнес-модели, но при этом не создавать высокий порог вхождения в крауд-отношения.

Не совсем понятным решением законодателя является установление ограничения на то, что лицом, привлекающим инвестиции, может быть только зарегистрированное в России юридическое лицо или индивидуальный предприниматель. Такой подход сразу сокращает количество потенциальных участников крауд-отношений, уменьшает возможность привлечения интересных и социально значимых проектов.

Исходя из вышеизложенного и не претендуя на полный анализ законодательного внедрения механизма краудфандинга в России, становится очевидным, что для более гибкого и благоприятного функционирования данной модели инвестирования следует более подробно на законодательном уровне урегулировать правовой статус лиц, участвующих в крауд-отношениях, в части прав и обязанностей, а также ответственности сторон.

Список литературы

1. Алилуева Н. А. Правовое регулирование краудфандинга и краудфандинговых площадок (платформ) // Инновационные технологии и технические средства для АПК: материалы Международной научно-практической конференции молодых ученых и специалистов, Воронеж, 14–16 ноября 2018 г. Воронеж: Воронежский государственный аграрный университет им. Императора Петра I. 2018. С. 539–543.

2. Кванина В. В., Спиридова А. В. Публично-правовое и частноправовое регулирование деятельности оператора инвестиционной платформы // Право и цифровая экономика. 2020. № 4 (10). С. 25–31.

3. Минина Н. В., Халецкий М. А., Крим М. М. Привлечение инвестиций с использованием инвестиционных платформ // Новации корпоративного законодательства. 2020. № 3. С. 6–13.

4. Патласов О. Ю. Краудфандинг: виды, механизм функционирования. Перспективы народного финансирования в России // Наука о человеке: гуманитарные исследования. 2015. № 2 (20). С. 209–219.

5. Правила оказания услуг по организации привлечения инвестиций с помощью инвестиционной платформы «fair finance p2b-платформа». URL: https://fairfin.ru/media/Правила_21.08.2021.pdf (дата обращения: 05.09.2022).

6. Разработана концепция регулирования краудфандинга в России / Банк России. URL: https://cbr.ru/press/event/?id=712 (дата обращения: 15.09.2022).

7. Реестр операторов инвестиционных платформ. URL: https://cbr.ru/vfs/registers/infr/list_invest_platform_op.xlsx (дата обращения: 10.09.2022).

8. Черняева А. К. Краудфандинг: понятие, особенности, и проблемы правового регулирования // VIA Scientiarum – Дорога знаний. 2018. № 2. С. 188–193.

В. В. Шумилова,
адъюнкт факультета подготовки
научно-педагогических и научных кадров,
Московский университет Министерства внутренних дел
Российской Федерации имени В. Я. Кикотя

ОБОРОТ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ: ЧАСТНОПРАВОВОЙ АСПЕКТ

Аннотация. В настоящей статье дается общее представление об обороте электронных денежных средств, которые являются важнейшим элементом современной платежной системы и необходимым объектом имущественного оборота, введение в него которых стало объективной потребностью для участников товарно-денежных отношений. В статье анализируются основные особенности оборота электронных денежных средств, связанные со спецификой осуществления их учета и перевода, а также акцентируется внимание на существующих правовых проблемах в рассматриваемой сфере, подчеркивается важность их решения.

Ключевые слова: электронные денежные средства, объект гражданских прав, имущественное право, денежный оборот, безналичный оборот, безналичные расчеты, средство платежа

ELECTRONIC MONEY FLOW: PRIVATE LAW ASPECT

Abstract. The article gives a general idea of the turnover of electronic money, which is an essential element of the modern payment system and a necessary object of property turnover, the introduction of which has become an objective need for participants in commodity-money relations. The article analyzes the main features of the turnover of electronic money associated with the specifics of their accounting and transfer, and also focuses on the existing legal problems in this area, emphasizes the importance of their solution.

Keywords: Electronic money, Object of civil rights, Thing in action, Money turnover, Non-cash turnover, Non-cash payments, Means of payment

Деньги прошли длительный период развития, который продолжается и сегодня. Масштабные преобразования в сфере денежного обращения, обусловленные внедрением электронных и информационных технологий, развитие цифрового сегмента экономики обусловили формирование в этих условиях новой формы организации расчетов – системы электронного денежного оборота, закономерным результатом чего стало и изменение самих экономических объектов и процессов, внедрение в оборот различных инновационных платежных технологий и, как следствие, введение в правовое поле новых правовых категорий. Это касается, прежде всего, появления в российской правовой системе такого объекта, как электронные денежные средства, которые являются наиболее перспективным продуктом в системе электронного платежного оборота, выступают его ядром и внедрение которых повлекло за собой формирование качественно ино-

го подхода к построению механизма денежного оборота. Так, М. А. Абрамова, отмечая высокую степень трансформации форм и механизмов оборота денег в эпоху широкого использования информационных сетей и распространения компьютерных технологий, указывает на формирование целостной концепции электронных денег, что обеспечивает их активное использование в денежном обороте [1. С. 213–218]. В этой связи комплексный анализ особенностей оборота электронных денежных средств имеет важное теоретическое и практическое значение.

Основной функцией, которую деньги выполняют в гражданском обороте, является функция средства платежа. В этих процессах, кроме наличных денег, в равной степени могут участвовать и иные платежные средства. Более того, в условиях развития экономических систем в парадигме тенденций глобализации товарно-денежных отношений традиционные деньги неспособны в полной мере выполнять свои функции в экономическом обороте, необходимые для обслуживания процессов реализации товаров и услуг. Появление электронных денежных средств, «выступающих инструментом оптимизации платежного оборота» [3. С. 7–13], стало в этой связи необходимым условием эффективного функционирования и использования имеющихся финансовых ресурсов.

Полноценное правовое регулирование операций с электронными денежными средствами началось с принятием Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – ФЗ № 161) и изданием в соответствии с ним иных нормативных актов. Данный закон, легализовав обращение электронных денежных средств на территории России и заложив основы механизма их регулирования, определил основные права и обязанности операторов электронных денежных средств, до этого основывавших свою деятельность преимущественно на общих диспозитивных нормах гражданского законодательства, описал порядок оказания платежных услуг, порядок перевода денежных средств, осуществляемого на основании договора, определил требования к порядку функционирования и деятельности организаций, осуществляющих операции с электронными денежными средствами и др.

Между тем российское законодательство не отвечает на вопрос, как эмитируются эти денежные средства (хотя понятием «эмиссия электронных денежных средств» законодатель не оперирует, этот термин прочно укоренился в данной отрасли в целях обозначения момента «появления» электронных денежных средств в электронных кошельках), не устанавливает порядок и условия выпуска электронных денежных средств в оборот, в нем не содержится описания механизма их оборота.

Преобладающей точкой зрения в сфере понимания правовой природы, гражданско-правовой сущности рассматриваемого явления, а также оснований и момента его возникновения как объекта гражданских прав является тезис о том, что электронные денежные средства – «права требования особого рода» [4. С. 14], функционирующие в гражданском обороте посредством безналичных расчетов: «…содержанием правоотношений, возникающих относительно оборота электронных денежных средств, как и при зачислении средств клиента на банковские счета, являются обязательственные права» [2. С. 15–19].

Необходимо также отметить, что электронные денежные средства способны обслуживать и нетоварные операции. На это указывает, во-первых, ст. 46 Налогового кодекса Российской Федерации (далее – НК РФ), анализ которой позволяет сделать вывод о том, что законодатель включает электронные денежные средства в состав имущества налогоплательщика, на которое может быть обращено взыскание в случае неуплаты или неполной уплаты налога в установленный срок; во-вторых, факт интеграции платежного сервиса «Яндекс.Деньги» (2016 г.) в Портал государственных услуг Российской Федерации. Данное событие позволило производить различные финансовые перечисления со стороны граждан в счет государства через электронный кошелек. В частности, гражданам стали доступны функции оплаты услуг жилищно-коммунального хозяйства, оплаты дорожных штрафов, оплаты государственных пошлин (например, за постановку автомобиля на учет в ГИБДД, за выдачу паспорта), ими можно погасить судебные и налоговые задолженности, а также осуществлять иные платежи.

Оборотоспособность электронных денежных средств не вызывает сомнений, однако имеет свои особенности, обусловленные их «виртуальной», обязательственно-правовой природой, связанные с некоторыми ограничениями с точки зрения правовых и технологических позиций.

Во-первых, особенностью механизма оборота электронных денежных средств является предоставление права на их выпуск только определенным кредитно-финансовым организациям.

Во-вторых, оборот данных идеальных объектов обеспечивается посредством обращения особого рода прав. Очевидно, что единственным способом правового оформления оборота электронных денежных средств может быть передача обязательственного права (п. 1 ст. 382, ст. 388 ГК РФ), которое позволяет его обладателю распоряжаться определенной суммой денег или денежных средств по своему усмотрению, возникающего из договора и существующего в форме уникальной записи в электронном кошельке об имеющихся в распоряжении средств до тех пор, пока они не примут свою прежнюю форму – форму наличных денег.

В-третьих, оборот электронных денежных средств и распоряжение ими является не просто актом волеизъявления субъекта товарообмена о приобретении соответствующего блага. Одного только намерения недостаточно для заключения сделки. Покупатель, он же клиент, должен сперва выразить его оператору, поскольку практическое осуществление операций по переводу электронных денежных средств возложено на него, выступающего третьим лицом в правоотношениях между продавцом и покупателем. Оно состоит в одновременном выполнении оператором трех последовательных действий: 1) получение распоряжения клиента о переводе денежных средств, 2) уменьшение остатка электронных денежных средств клиента (плательщика), 3) увеличение остатка электронных денежных средств получателя денежных средств. При этом инициирование платежа может принадлежать как плательщику, так и получателю (взыскателю) средств. Так, анализ ст. 46 НК РФ позволяет сделать выводы о том, что законодатель включает электронные денежные средства в состав имущества налогоплательщика, на ко-

торое может быть обращено взыскание в случае неуплаты или неполной уплаты налога в установленный срок. На это также указывает ст. 27 ФЗ «О банках и банковской деятельности, которая предусматривает возможность взыскания остатка электронных денежных средств.

В-четвертых, осуществление операций по распоряжению электронными денежными средствами возможно исключительно с использованием электронного средства платежа (п. 19 ст. 3 ФЗ № 161-ФЗ).

В-пятых, субъекты дистанционного предпринимательства не могут осуществлять платежи посредством системы электронных денежных средств, но могут принимать их от потребителей товаров, работ и услуг (п. 9 ст. 7. ФЗ № 161-ФЗ).

Дополнительно в законодательстве содержатся положения, устанавливающие правовые ограничения на размер суммы, доступной в электронном кошельке, а также определяющие пределы объема осуществляемых переводов.

Резюмируя изложенное, нельзя не отметить, что, несмотря на то, что место электронных денежных средств в системе объектов гражданских прав в настоящее время остается дискуссионным вопросом, их введение в безналичный денежный оборот создает необходимость осмысления их правовой природы, выделения признаков, позволяющих отделить их от иных объектов гражданских прав, а также решения правовых проблем, возникающих в связи с их вовлечением в этот оборот. Оборот электронных денежных средств с точки зрения теории гражданского права осуществляется в рамках применяемых форм безналичных расчетов (п. 19 ст. 3 ФЗ № 161-ФЗ) и представляет собой процесс движения денежных средств, возникающих из обязательственной связи его субъектов, посредством их перевода во исполнение частноправовых или публично-правовых обязанностей их «владельцев», а также по иным основаниям.

Список литературы

1. Абрамова М. А. Формирование современной концепции денег в контексте нового качества экономики // Научные труды Вольного экономического общества России. 2019. № 4. С. 213–218.

2. Дерюгина Т. В., Чеговадзе Л. А. Правовая природа электронных денежных средств // Материалы Весенней международной научно-практической сессии Института права: Международного круглого стола «Умные технологии правового обеспечения конкурентоспособной предпринимательской среды», Международной научно-практической конференции «Судопроизводство в Российской Федерации и за рубежом: вопросы истории и проблемы совершенствования». Волгоград. 2021. № 3. С. 15–19.

3. Достов В. Л., Кузнецов В. А., Шуст П. М. Электронные деньги как инструмент оптимизации платежного оборота // Деньги и кредит. 2013. № 12. С. 7–13.

4. Коростелев М. А. Правовой режим электронных денег в гражданском законодательстве: дис. … канд. юрид. наук. Москва, 2015. 229 с.

А. Ю. Яковлева-Чернышева,
доктор экономических наук, доцент,
Сочинский филиал Всероссийского государственного
университета юстиции

ПРОБЛЕМНЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ГРАЖДАНСКОМ ОБОРОТЕ

Аннотация. Целью исследования в данной статье является анализ проблемных аспектов правового регулирования цифровых технологий в гражданском обороте. Обоснована актуальность развития нормативной правовой базы в данной сфере, исходя из потребности построения модели правового регулирования цифрового общества, ключевая роль в которой отводится гражданскому законодательству. Особое внимание уделено смарт-контрактам как одной из наиболее перспективных цифровых технологий, применяемых в гражданском обороте.

Ключевые слова: цифровое общество, гражданское право, договорное право, гражданский оборот, цифровые технологии, смарт-контракты, блокчейн

PROBLEMATIC ASPECTS OF LEGAL REGULATION OF DIGITAL TECHNOLOGIES IN CIVIL CIRCULATION

Abstract. The purpose of the study in this article is the analysis of problematic aspects of legal regulation of digital technologies in civil circulation. The urgency of the development of the normative legal framework in this sphere has been substantiated, based on the need to build a model of legal regulation of the digital society, in which a key role is assigned to the civilian legislation. Special attention is paid to smart contracts as one of the most promising digital technologies used in civil circulation.

Keywords: Digital society, Civil law, Contract law, Civil turnover, Digital technology, Smart contracts, Blockchain

Цифровые технологии проникли практически во все сферы жизни современного общества, что позволяет обоснованно использовать термин «цифровое общество». Не вызывает сомнений, что цифровое общество нуждается в построении соответствующей модели правового регулирования [13. С. 8]. При этом необходимо учитывать, что цифровые технологии стремительно внедряются «не только в науку, производство, образование, управленческую деятельность, но и в повседневный массовый обиход» [10. С. 19]. Логичным представляется вывод, что «в самом ближайшем будущем личность во всех своих проявлениях будет окончательно встроена в цифровое пространство» [11]. В свою очередь, это потребует адекватного урегулирования гражданских правоотношений в условиях новой реальности.

Значимость развития нормативно-правовой базы в целях регулирования цифровых технологий в гражданском обороте подчеркнул В. В. Путин в послании Федеральному Собранию РФ от 20.02.2019. В своем выступлении он обратил внимание на первоочередную необходимость принятия новых законов «для создания правовой среды новой, цифровой экономики, которые позволят заключать гражданские сделки…» [3].

Таким образом, гражданское законодательство является ключевым компонентом формируемой системы правового регулирования цифрового общества. Исходя из этого, исследование проблемных аспектов правового регулирования цифровых технологий в гражданском обороте характеризуется высоким уровнем актуальности.

В России, как и в других странах мира, предпринимаются шаги со стороны государства, связанные с развитием нормативной правовой базы, регулирующей цифровые технологии в гражданских правоотношениях. Среди кардинальных изменений необходимо выделить поправки в Гражданский кодекс Российской Федерации (далее – ГК РФ), которые были внесены Федеральным законом от 18.03.2019 № 34-ФЗ [2]. В частности, было урегулировано применение электронного документооборота в целях заключения и исполнения гражданско-правовых договоров.

В условиях цифровизации гражданского оборота договорное право обоснованно получает дальнейшее развитие, так как договор является значимым актом правоприменения в сфере гражданско-правовых отношений. Договор, во-первых, служит основой для возникновения прав и обязанностей, во-вторых, выступает в качестве регулятора правоотношений [5. С. 22]. Однако до сих пор в области договорного права остаются незаполненные пробелы. Так, несмотря на то, что понятие и правовая природа смарт-контрактов уже несколько лет находятся в центре внимания правоведов, в российской юридической науке нет единого понимания по данным вопросам, а правовое регулирование применения смарт-контрактов не нашло своего места в российском гражданском законодательстве. При этом понятие «смарт-контракт», означающее в переводе «умный контракт», на сегодняшний день вошло в законодательство ряда стран. Его всесторонне изучают ученые, которые используют различные подходы, опирающиеся на технологические или правовые характеристики умных контрактов. Кроме того, смарт-контракты достаточно широко применяются на практике [9. С. 33].

Впервые понятие «смарт-контракт» появилось в 1994 г., когда его ввел в научный обиход ученый из США Н. Сабо, предложивший следующее определение: «Компьютеризированный транзакционный протокол, который исполняет условия договора» [17].

На уровне законодательства термин «смарт-контракт» впервые был введен в Италии. В Законе «О срочных положениях в отношении поддержки и упрощения системы ведения бизнеса и государственного управления», принятом в 2019 г., смарт-контракт трактуется как компьютерная программа, создаваемая с помощью технологии распределенного реестра и легально используемая двумя и более сторонами согласно ранее заключенным соглашениям [8].

В исследовании о смарт-контрактах Люксембургской ассоциации блокчейна и технологии распределенного реестра, опубликованном в июле 2021 г., дано определение, характеризующее смарт-контракт как автоматизированный протокол сделки, заключаемой между двумя или более сторонами, который может быть самоисполняемым либо представлять собой юридически обязывающий договор при условии соблюдения требований применимого права [16. С. 448–449].

В аналитическом обзоре Банка России 2018 г., во-первых, дано определение смарт-контракта, трактуемого как договор, «в котором часть или все условия за-

писываются, исполняются и/или обеспечиваются компьютерным алгоритмом автоматически в специализированной программной среде» [4. С. 3], во-вторых, перечислены технологические характеристики умных контрактов [4. С. 4–5].

Анализ технологических аспектов применения смарт-контрактов позволяет выявить как положительные, так и отрицательные последствия их внедрения в гражданский оборот. На наш взгляд, преимуществами умных контрактов в первую очередь являются такие их характеристики, как самоисполняемость и невозможность внесения каких-либо корректировок без согласования сторонами. Что касается проблем, то, как отмечается в научной литературе, для создания смарт-контракта необходимо привлекать опытного программиста, но даже это не гарантирует допущения ошибок в написании программного кода [14. С. 53]. Поэтому мы согласны с точкой зрения, согласно которой проблемы могут возникнуть при вполне вероятной ситуации каких-либо сбоев в работе программного обеспечения, когда понадобится решать вопрос о распределении ответственности [6].

Решение указанной выше и других возможных проблем, связанных с применением смарт-контрактов, лежит в правовом поле, требуя проведения научных разработок и внесения изменений в нормативные правовые акты. Пока что в российском законодательстве понятие смарт-контрактов отсутствует, а в доктрине представлены различные подходы к пониманию правовой сущности умного контракта, согласно которым он является специфическим видом, способом заключения, способом исполнения договора, способом обеспечения исполнения обязательств по заключенному договору и др. [7, 12, 14, 15].

Ликвидация пробелов в законодательстве возможна лишь в случае выбора одного из перечисленных выше подходов, поскольку каждый из них предполагает различные механизмы урегулирования использования умных контрактов в гражданском обороте. К примеру, в случае признания смарт-контракта специфическим видом договора его регулирование должно основываться на положениях 1 части ГК РФ, поскольку специальные нормы отсутствуют. Другие положения гражданского законодательства будут задействованы, если рассматривать смарт-контракт не как вид договора, а как специфический способ его заключения, отличительной характеристикой которого является использование технологии распределенного реестра (блокчейна) в качестве одного из способов заключения договора в электронной форме, и т. д.

По нашему мнению, важнейшей характеристикой умных контрактов с позиций договорного права является их самоисполняемость. В связи с этим мы считаем, что смарт-контракты являются специфическим способом исполнения обязательств, который находит свое применение при заключении договора в электронной форме, предусматривающего автоматизированное исполнение обязательств в рамках технологии распределенного реестра (блокчейна) [16. С. 451]. При этом в действующей редакции ст. 309 ч. 2 ГК РФ предусмотрено автоматизированное исполнение обязательств по договору [1], что не исключает возможности применения для этих целей смарт-контрактов. Однако этого недостаточно, поскольку сохраняются различные вопросы, требующие надлежащего урегулирования. Большая часть из них связана со способами защиты прав и законных интересов сторон договоров, заключаемых с применением смарт-контрактов.

Таким образом, на современном этапе развития гражданских правоотношений цифровые технологии получили достаточно широкое распространение и имеют значительный потенциал для дальнейшего развития. Одним из перспективных направлений применения цифровых технологий в гражданском обороте являются смарт-контракты. Однако ни в законодательстве, ни в доктрине нет определения понятия смарт-контрактов, единого подхода к пониманию их правовой природы и четко прописанных механизмов правового регулирования. Следовательно, заполнение данного пробела в законодательстве является одним из насущных вопросов совершенствования правового регулирования цифровых технологий в гражданском обороте.

Список литературы

1. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 01.07.2021, с изм. от 08.07.2021) (с изм. и доп., вступ. в силу с 01.01.2022). URL: http://www.consultant.ru/document/cons_doc_LAW_9027/ (дата обращения: 24.06.2022).

2. Федеральный закон от 18.03.2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_320398/ (дата обращения: 24.06.2022).

3. Послание Президента Российской Федерации Федеральному Собранию Российской Федерации от 20.02.2019 «О положении в стране и основных направлениях внутренней и внешней политики государства». URL: http://www.kremlin.ru/acts/bank/44032 (дата обращения: 25.06.2022).

4. Аналитический обзор по теме «Смарт-контракты» / Банк России. URL: https://cbr.ru/Content/Document/File/47862/SmartKontrakt_18–10.pdf (дата обращения: 25.06.2022).

5. Ахмедов А. Я. К вопросу о признаках смарт-контракта как договорной конструкции // Право и цифровая экономика. 2020. № 2. С. 22–25.

6. Вызов цифровой экономики: смарт-контракты и цифровые права. URL: https://zakon.ru/blog/2019/05/20/vyzov_cifrovoj_ekonomiki_smart-kontrakty_i_cifrovye_prava (дата обращения: 25.06.2022).

7. Ефимова Л. Г., Михеева И. Е., Чуб Д. В. Процессуальные аспекты использования смарт-контрактов в гражданском обороте по праву России и зарубежных стран // Вестник гражданского процесса. 2020. Т. 10, № 4. С. 235–253.

8. Крысенкова Н. Б. Смарт-контракты в иностранном правовом пространстве. URL: https://urfac.ru/?p=2730#_ftn3 (дата обращения: 25.06.2022).

9. Лисица В. Н., Зайнутдинова Е. В. Цифровые права и их использование в смарт-контракте // Юридическая наука и практика. 2022. Т. 18, № 1. С. 29–38.

10. Разуваев Н. В. Цифровая трансформация субъективных гражданских прав: проблемы и перспективы // Теоретическая и прикладная юриспруденция. 2021. № 1 (7). С. 18–38.

11. Сарбаш С. Гражданский оборот в цифровую эпоху. URL: https://zakon.ru/blog/2017/10/21/grazhdanskij_oborot_v_cifrovuyu_epohu (дата обращения: 29.06.2022).

12. Сомова Е. В. Смарт-контракт в договорном праве // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 2 (75). С. 79–86.

13. Трансформация права в цифровую эпоху: монография / Министерство науки и высшего образования РФ, Алтайский государственный университет; под ред. А. А. Васильева. Барнаул: Изд-во Алт. ун-та, 2020. 432 с.

14. Фазлиева Л. К., Рахимов Э. Х. Смарт-контракт в гражданско-правовом обороте // Вестник Уфимского юридического института МВД России. 2021. № 2 (92). С. 52–57.

15. Чурилов А. Ю. Смарт-контракты и принципы обязательственного права // Правовая парадигма. 2021. Т. 20, № 1. С. 113–117.

16. Яковлева-Чернышева, А. Ю. Смарт-контракты: понятие и проблемы гражданско-правового регулирования // Интеллектуальный капитал и цифровая трансформация общества: сб. науч. ст. Минского филиала РЭУ им. Г. В. Плеханова; редкол.: А. Б. Елисеев, И. А. Маньковский (гл. ред.). Минск: БГАТУ, 2022. С. 447–453.

17. Szabo N. The Idea of Smart Contracts. 1994. URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (дата обращения: 25.06.2022).

СОДЕРЖАНИЕ | CONTENTS

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЙ | DIGITAL TECHNOLOGIES IN THE SYSTEM OF CRIMINAL LAW RELATIONS

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ МЕЖДУНАРОДНО-ПРАВОВЫХ ОТНОШЕНИЙ | DIGITAL TECHNOLOGIES IN THE SYSTEM OF INTERNATIONAL LEGAL RELATIONS

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ЧАСТНОПРАВОВЫХ (ЦИВИЛИСТИЧЕСКИХ) ОТНОШЕНИЙ | DIGITAL TECHNOLOGIES IN THE SYSTEM OF PRIVATE LAW (CIVIL) RELATIONS

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
I Международной научно-практической конференции

23 сентября 2022 г.
г. Казань

В шести томах
Том 2

Под редакцией И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой

Главный редактор *Г. Я. Дарчинова*
Редакторы: *Г. А. Тарасова, Е. А. Маннапова*
Технический редактор *О. А. Аймурзаева*
Дизайн обложки: *Г. И. Загретдинова*

ISBN 978-5-8399-0769-0

9 785839 907690

Подписано в печать 27.10.2022. Формат 60×84/16.
Гарнитура PT Astra Serif, 9. Усл. печ. л. 32,32. Уч.-изд. л. 26,67.
Тираж 2000 экз. Заказ № 108.

Издательство «Познание» Казанского инновационного университета им. В. Г. Тимирясова
420111, г. Казань, ул. Московская, 42; тел. (843) 231-92-90; e-mail: zaharova@ieml.ru

Отпечатано с готового оригинал-макета в типографии ООО «ТЦО «Таглимат»
420108, г. Казань, ул. Зайцева, 17

НАУРР
Национальная Ассоциация Участников Рынка Робототехники

ICTONLINE

ICT2GO

УВЕРЕННОСТЬ В КАЖДОМ РЕШЕНИИ
ГАРАНТ
ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

ХАЙТЕК

it·world

technovery

International Journal of Law in Changing World

РАПСИ Российское агентство правовой и судебной информации

IP CLUB