



ЦИФРОВЫЕ
ТЕХНОЛОГИИ
И ПРАВО

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

СБОРНИК НАУЧНЫХ ТРУДОВ
I МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ
КОНФЕРЕНЦИИ

В шести томах

Том 6

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. Бегешева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 472 с. EDN: PWHXPZ. DOI: http://dx.doi.org/10.21202/978-5-8399-0773-7_2022_6_472

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. 6. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2022. – 472 p. EDN: PWHXPZ. DOI: http://dx.doi.org/10.21202/978-5-8399-0773-7_2022_6_472



Казанский
инновационный
университет имени
В. Г. Тимирязова



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

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
I Международной научно-практической конференции

г. Казань, 23 сентября 2022 г.

В шести томах

Том 6



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 6

УДК 004:34(063)

ББК 67с51я43

Ц75

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

Редакторы:

И. Р. Бегишев, доктор юридических наук, заслуженный юрист Республики Татарстан, главный научный сотрудник Научно-исследовательского института цифровых технологий и права, профессор кафедры уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирязова;

Е. А. Громова, кандидат юридических наук, доцент, заместитель директора Юридического института по международной деятельности, доцент кафедры предпринимательского, конкурентного и экологического права Южно-Уральского государственного университета;

М. В. Залоило, кандидат юридических наук, ведущий научный сотрудник отдела теории права и междисциплинарных исследований законодательства Института законодательства и сравнительного правоведения при Правительстве Российской Федерации;

И. А. Филипова, кандидат юридических наук, доцент, доцент кафедры трудового и экологического права Национального исследовательского Нижегородского государственного университета имени Н. И. Лобачевского;

А. А. ШUTOVA, кандидат юридических наук, старший научный сотрудник Научно-исследовательского института цифровых технологий и права, доцент кафедры уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирязова

Рецензенты:

А. К. Жарова, доктор юридических наук, доцент, директор Центра исследований киберпространства, ассоциированный член международного научно-образовательного центра «Кафедра ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам» Национального исследовательского университета «Высшая школа экономики»;

А. В. Минбалева, доктор юридических наук, доцент, заведующий кафедрой информационного права и цифровых технологий Московского государственного юридического университета имени О. Е. Кутафина;

Э. В. Талапина, доктор юридических наук, доктор права (Франция), ведущий научный сотрудник Центра технологий государственного управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации;

Ю. С. Харитонова, доктор юридических наук, профессор, руководитель Центра правовых исследований искусственного интеллекта и цифровой экономики, профессор кафедры предпринимательского права Московского государственного университета имени М. В. Ломоносова

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. Громова, М. В. Залоило, И. А. Филиповой, А. А. ШUTOVA. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – 472 с. EDN: PWNXPZ. DOI: http://dx.doi.org/10.21202/978-5-8399-0773-7_2022_6_472

ISBN 978-5-8399-0767-6

ISBN 978-5-8399-0773-7 (Том 6)

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 режимом 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 обобщают в формате мультидисциплинарного «хакатона» взгляды и подходы молодых ученых и специалистов из различных областей знаний к экономическим, социальным, политическим, юридическим и иным проблемам цифровой трансформации.

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 978-5-8399-0773-7 (Том 6)

© Авторы, 2022

© Казанский инновационный университет
имени В. Г. Тимирязова, 2022

UDC 004:34(063)
LBC 67c51я43

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

Editors:

Ildar R. Begishev, Doctor of Law, Honored Lawyer of the Republic of Tatarstan, Chief Researcher of Scientific-Research Institute of Digital Technologies and Law, Professor of the Department of Criminal Law and Procedure, Kazan Innovative University named after V.G. Timiryasov;

Elizaveta A. Gromova, PhD (Law), Associate Professor, Deputy Director of the Law Institute on international activity, Associate Professor of the Department of Entrepreneurial, Competition and Environmental Law, South Ural State University;

Maksim V. Zaloilo, PhD (Law), Leading Researcher, Department of the Theory of Law and Interdisciplinary Research of Legislation, Institute of Legislation and Comparative Law under the Government of the Russian Federation;

Irina A. Filipova, PhD (Law), Associate Professor, Associate Professor of the Department of Labor Law and Environmental Law, National Research Lobachevsky State University of Nizhny Novgorod;

Albina A. Shutova, PhD (Law), Senior Researcher of Scientific-Research Institute of Digital Technologies and Law, Associate Professor, Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov

Reviewers:

Anna K. Zharova, Doctor of Law, Associate Professor, Director of the Center for Cyberspace Research, Associate member of the International scientific-educational Center “UNESCO Chair on Copyright, Neighboring, Cultural and Information Rights”, National Research University Higher School of Economics;

Aleksey V. Minbaleev, Doctor of Law, Associate Professor, Head of the Department of Informational Law and Digital Technologies, Kutafin Moscow State Law University;

Elvira V. Talapina, Doctor of Law, Doctor of Law (France), Chief Researcher of the Institute of State and Law of the Russian Academy of Sciences, Leading Researcher of the Center for Public Governance Technologies, Russian Presidential Academy of National Economy and Public Administration;

Yuliya S. Kharitonova, Doctor of Law, Professor, Head of the Center for Legal Research of Artificial Intelligence and Digital Economy, Professor of the Department of Entrepreneurial Law, Lomonosov Moscow State University

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. 6. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2022. – 472 p. EDN: JSIXFM. DOI: http://dx.doi.org/10.21202/978-5-8399-0773-7_2022_2_472

ISBN 978-5-8399-0767-6

ISBN 978-5-8399-0773-7 (Volume 6)

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 summarize, in the format of a multidisciplinary “hackathon”, the attitudes and approaches of young scientists and specialists from various fields of knowledge to economic, social, political, legal and other issues of digital transformation.

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

© Authors, 2022

© Kazan Innovative University named after V. G. Timiryasov, 2022

ISBN 978-5-8399-0767-6

ISBN 978-5-8399-0773-7 (Volume 6)

МУЛЬТИДИСЦИПЛИНАРНЫЕ АСПЕКТЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

З. А. Айларова,

студент,

Владикавказский филиал Финансового университета
при Правительстве Российской Федерации

ВЛИЯНИЕ ЦИФРОВОГО СЛЕДА НА ПОВСЕДНЕВНУЮ И ПРОФЕССИОНАЛЬНУЮ ДЕЯТЕЛЬНОСТЬ

Аннотация. В современных экономических условиях использование информационных, инновационных и сетевых технологий позволяет сделать доступной разную информацию, продукцию, услуги. У каждого пользователя гаджетами и интернет-технологиями накапливается цифровой след, способный оказать влияние на разные сферы жизни и деятельности. В данной статье приводится обзорное исследование понятия цифрового следа, средств его защиты и статистики преступлений, совершенных с использованием информационных технологий. Показана необходимость регулирования пользователями своего цифрового следа.

Ключевые слова: информационные технологии, цифровые технологии, мобильные технологии, цифровая экономика, цифровой след, Интернет, киберпреступления, защита информации

THE IMPACT OF THE DIGITAL FOOTPRINT ON EVERYDAY AND PROFESSIONAL ACTIVITIES

Abstract. In modern economic conditions, the use of information, innovation and network technologies makes it possible to make various information, products, and services available. Each user of gadgets and Internet technologies accumulates a digital footprint that can affect different areas of life and activity. This article provides an overview study of the concept of a digital footprint, means of its protection and statistics of crimes committed using information technology. The need for users to regulate their digital footprint is shown.

Keywords: Information technology, Digital technology, Mobile technology, Digital economy, Digital footprint, Internet, Cybercrime, Information security

В настоящее время в России проходит активное внедрение современных цифровых технологий не только в профессиональную, но и в повседневную деятельность каждого человека. Реализация направлений национальной программы «Цифровая экономика Российской Федерации» [8] предполагает цифровизацию экономики, управления, инфраструктуры, образования, сферы услуг и т. д. В связи с этим большое количество потребностей общества удовлетворяется с использованием информационных, цифровых, сетевых, мобильных, облачных и других инновационных технологий [9. С. 106–123]. Большинство рабочих и бытовых вопросов может быть решено с помощью мобильных телефонов, планшетов, компьютеров

и других гаджетов [2. С. 135–138]. Однако повсеместное использование цифровых устройств приводит к некоторым последствиям, которые необходимо учитывать в дальнейшей деятельности.

Одним из побочных результатов цифровизации является эффект цифровых следов. Цифровые следы (далее – следы) – это совокупность действий, используемых в Интернете и на других платформах, необходимых для просмотра и использования веб-страниц [5. С. 64–70; 10. С. 29–32].

Цифровой след (цифровая тень, электронный след) представляет собой набор данных, оставляемых пользователем при использовании сетевых технологий [11. С. 161–165]. Эти данные отражают посещаемые сайты, отправляемый контент, данные онлайн-форм и т. д. Такие следы могут быть использованы с целью мониторинга действий человека и его устройство в Сети [6. С. 415–419]. На рис. 1 приведена краткая характеристика типов цифровых следов [5. С. 64–70; 9. С. 106–123].

Активный цифровой след	Пассивный цифровой след
<p>Пользователь оставляет активный цифровой след, когда намеренно делится информацией о себе: делает публикации в социальных сетях или оставляет сообщения на сайтах или онлайн-форумах. Если пользователь вошел на веб-сайт с использованием зарегистрированного имени или профиля, все опубликованные им сообщения будут составлять его активный цифровой след. Также активный цифровой след остается при заполнении онлайн-форм, например, подписке на информационные рассылки, или при согласии принимать файлы cookie в браузере.</p>	<p>Пассивный цифровой след создается, когда информация о пользователе собирается без его ведома. Это происходит, например, когда на веб-сайте собирается информация о том, сколько раз пользователи посещали сайт, откуда эти пользователи и их IP-адреса. Это скрытый процесс, о котором пользователи могут не догадываться. Другим примером использования пассивного следа является анализ рекламодателями ваших лайков, репостов и комментариев в социальных сетях с целью последующего профилирования и отображения вам определенного контента.</p>

Рис. 1. Типы следов и их характеристика

Цифровые следы отличаются от социальных сетей тем, что в соцсетях пользователь сам добровольно публикует информацию о себе (увлечения, местоположения, интересы и т. д.) и использование этих данных без ведома пользователя практически невозможно.

Использование следа дает возможность не только использовать, но и сохранять, копировать и передавать информацию о конкретном пользователе другим пользователям. Например, воспользоваться следом могут при приеме на работу или в учебное заведение [1. С. 232–236; 5. С. 64–70]. В связи с этим очевидно то, что цифровые следы не являются безопасными и требуется защита от неправомерного использования другими пользователями Интернета [3. С. 118–125]. Основой защиты цифрового следа являются мероприятия, которые помогут сократить следы пользователя. На рис. 2 представлены рекомендации по защите следа [2. С. 135–138; 4. С. 110–112].

На увеличение цифрового следа пользователя существенное влияние оказывает развитие цифровых экосистем на основе использования гаджетов и новых приложений. 2021 г. считается «рекордным» по количеству использования гаджетов [12]. Одной из

причин такого роста стала пандемия COVID-19. Для сравнения в 2019 г. в России мобильные телефоны использовали 33 % населения, смартфоны – 59 %, 8 % – ни первое, ни второе. В 2021 г. использование соцсетей через гаджеты увеличилось и составило 67,8 % населения, что на 5,1 % больше, чем в 2020 г. Использование Интернета в 2021 г. увеличилось по сравнению с предыдущим годом и составило 85 % населения.

Использовать поисковые системы для проверки своего цифрового следа	Уменьшить количество источников, упоминающих ваше имя	Ограничить объем предоставляемых данных	Проверить параметры конфиденциальности
Ограничить раскрытие излишней информации в социальных сетях	Избегать незащищенные веб-сайты	Не указывать личные данные при использовании публичных сетей Wi-Fi	Удалять старые учетные записи
Создать надежные пароли	Не выполнять авторизацию через соцсети	Поддерживать актуальность программного обеспечения	Настроить параметры использования мобильного устройства
Сохранять конфиденциальность медицинских документов	Оценивать материалы перед публикацией	В случае взлома принять немедленные меры	Использовать VPN

Рис. 2. Способы защиты цифрового следа пользователем

Таким образом, использование современных гаджетов в профессиональной и повседневной деятельности оставляет цифровые следы пользователей, которые могут копироваться, сохраняться, передаваться и использоваться другими пользователями Интернета не только в России, но и во всем мире. В связи с этим актуальным является исследование влияния цифровых следов на общество. В данной работе обзор влияния цифровых следов на профессиональную деятельность проведен на примере использования ИТ в экономической сфере.

В современных экономических условиях развитие инновационных технологий оказывает огромное влияние на экономическую сферу, опережая все другие отрасли жизни общества. В 2019–2021 гг. цифровые технологии оказывали большое влияние на такие сектора экономики, как розничная торговля, туризм и др. [13. С. 76–78].

Цифровая экономика (далее – ЦЭ) – это коммерческая деятельность, связанная с продажей товаров, работ, услуг через онлайн-сервисы и интернет-платформы. Следовательно, можно говорить об использовании имеющихся бизнес-моделей. Благодаря использованию ИТ-технологий стало возможным подключение поставщиков, подрядчиков, покупателей и других участников напрямую, без посредников [14. С. 137–148; 15]. Главным звеном развития ЦЭ является информация – главный экономический информационный продукт, который хранится в цифровых сервисах и платформах, передается другим пользователям с помощью цифровых технологий.

Развитие ЦЭ направлено на удовлетворение запросов потребителей, качество и цену товара, продукции, услуг. ЦЭ может полностью изменить информационный

рынок не только в России, но и во всем мире. Именно благодаря внедрению и развитию цифровых технологий российские организации малого и среднего бизнеса могут конкурировать не только между собой, но и с крупными международными организациями [13. С. 76–78]. Ярким примером этого является информационная модель строительства – BIM (Building Information Modeling). Именно благодаря использованию этой модели стало возможным одновременное использование проектирования и строительства, ремонт и эксплуатация объектов строительной отрасли.

Однако внедрение, использование и развитие ИТ в экономике приводит к увеличению числа финансовых преступлений, в основном связанные с использованием электронных валют. По данным Росстата [12], в 20 % случаев расследования экономических преступлений назначается проведение компьютерных экспертиз. Многие организации осуществляют бухгалтерский учет и финансовый контроль в электронном виде, которые возможно отследить с помощью цифровых следов, доступных киберпреступникам. За 2021 г. в сфере компьютерной информации сотрудниками правоохранительных органов на территории России зарегистрировано 517 722 случаев ИТ-преступлений, в 2020 г. – 510 396, в 2019 г. – 294 409. Наблюдается существенный рост ИТ-преступлений, в том числе на основе цифровых следов. На рис. 3 приведена статистика количества финансовых преступлений [12]. Видна отрицательная динамика: в 2021 г. число финансовых преступлений увеличилось на 72 %, совершенных с использованием ИТ – на 113 %. Безусловно, это связано с увеличением количества пользователей гаджетами на основе интернет-технологий [2. С. 135–138; 7. С. 709–713].



Рис. 3. Статистика финансовых преступлений за 2020–2021 гг.

Таким образом, внедрение и развитие современных цифровых технологий обработки информации в повседневной жизни и профессиональной деятельности каждого человека влечет за собой увеличение цифрового следа. Цифровизация разных сфер деятельности направлена на повышение объемов цифровых операций, а особенно предоставления товаров, работ, услуг на базе дистанционных технологий. Это также способствует увеличению следов. Цифровые следы могут использоваться для отслеживания действий человека и его устройств с использованием Интернета. Например, при приеме на работу специальные службы по подбору персонала используют цифровой след претендента для составления собственного резюме о кандидате на вакансию. Однако следы могут заинтересовать других

пользователей возможностью наживы. В настоящее время количество преступлений с использованием ИТ существенно возрастает. В связи с этим в перспективе необходимо провести анализ наиболее уязвимых данных в цифровых следах, обзор законодательной базы в сфере киберпреступности, уточнить рекомендации по защите цифровых следов пользователей в конкретных сферах.

Список литературы

1. Айларова З. А., Санагоева Д. К. Проблемы занятости молодежи в РСО-Алания // Молодежь и наука: актуальные проблемы социально-экономического развития регионов России: материалы VIII Всероссийской научно-практической конференции приуроченной к 90-летию Владикавказского филиала Финансового университета при Правительстве Российской Федерации. 2020. С. 232–236.

2. Барченкова Я. В. Цифровые следы при расследовании мошенничества, совершенного при помощи средств сотовой связи // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2020. № 4. С. 135–138.

3. Барышкин Н. В., Копышева Т. Н. Нормативно-справочная основа защиты информации в государственных органах власти // Актуальные проблемы математических и технических наук: сборник научных статей. 2015. С. 118–125.

4. Батчаева З. Б., Хачирова Ф. М., Уртеннова К. К., Кундохова К. Р. Обеспечение информационной безопасности и защита персональных данных // Тенденции развития науки и образования. 2021. № 79–1. С. 110–112.

5. Каткова Д. А. «Цифровой след» в системе составления цифрового портрета для подбора персонала // Гуманитарный научный журнал. 2021. № 3. С. 64–70.

6. Козаева К. Г., Плиева В. А., Волик М. В. Информационная безопасность: контроль персонала // Молодежь и наука: актуальные вопросы социально-экономического развития регионов России: материалы Всероссийской научно-практ. конф., посвященной 95-летию Финансового университета при Правительстве Российской Федерации. 2014. С. 415–419.

7. Кулаков В. Д. Цифровые следы финансовых преступлений: особенности назначения и производства экспертизы // Научный аспект. 2020. Т. 5, № 2. С. 709–713.

8. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). URL: https://www.consultant.ru/document/cons_doc_LAW_328854/ (дата обращения: 25.07.2022).

9. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123.

10. Рустикова Г. С. Информационная безопасность электронного обучения: цифровые следы и цифровая тень обучаемых // Информационное право. 2019. № 3. С. 29–32.

11. Тотикова А. А., Волик М. В. Интернет и его основные виды сервиса // Экономические, финансовые и управленческие аспекты внедрения цифровых технологий: сборник статей и тезисов докладов XXIII Международной научно-практ. конф. 2019. С. 161–165.

12. Федеральная служба государственной статистики. Официальный сайт. URL: <https://rosstat.gov.ru/> (дата обращения: 25.07.2022).

13. Ципинова А. С., Дзусова И. Г., Волик М. В. Интернет-технологии и их роль в бизнесе // Гуманитарные и социально-экономические науки. 2020. № 2 (111). С. 76–78.

14. Rodriguez M., Boyer S. The impact of mobile customer relationship management (mCRM) on sales collaboration and sales performance // Journal of Marketing Analytics. 2020. № 8 (3). С. 137–148.

15. Volik M. Features of the analysis of business processes of the company (on the example of customer service in a travel agency) // SPBPU IDE '19: Proceedings of the 2019 International SPBPU Scientific Conference on Innovations in Digital Economy. 2019. P. 3373505.

Н. В. Алексеев,
старший преподаватель,
Брянский государственный университет
имени академика И. Г. Петровского

КОНЦЕПЦИЯ ТВОРЧЕСКОГО СТИЛЯ В ЭПОХУ НЕЙРОСЕТЕВОГО ИСКУССТВА

Аннотация. Проблематика влияния технологии искусственного интеллекта на право с некоторых пор стала актуальна для юридических исследований. В настоящей работе исследуется влияние феномена искусственного интеллекта на творческую деятельность человека и ее результаты. Способность технологии искусственного интеллекта имитировать творческую деятельность человека и «подражать» творческому почерку конкретных авторов и исполнителей будет вытеснять человека из креативной сферы. В статье говорится о необходимости защиты уникального творческого стиля авторов и исполнителей. В контексте быстрого развития технологий эта идея будет приобретать значение, поскольку в этом заинтересованы как сами авторы и исполнители, рискующие быть замещенными машиной, так и их аудитория. Автор высказывает предположение о создании института авторского права, который бы юридически ограничил возможность копирования уникального творческого стиля при помощи технологии искусственного интеллекта.

Ключевые слова: искусственный интеллект, авторское право, творческий стиль, автор, исполнитель, творческая деятельность, квази-произведение

THE CONCEPT OF CREATIVE STYLE IN THE AGE OF NEURAL NETWORK ART

Abstract. The problem of the impact of artificial intelligence technology on the law has become relevant for legal research for some time now. In this paper, we study the influence of the phenomenon of artificial intelligence on human creative activity and its results. The ability of artificial intelligence technology to imitate the creative

activity of a person and “imitate” the creative style of specific authors and performers will force a person out of the creative sphere. The article talks about the need to protect the unique creative style of authors and performers. In the context of the rapid development of technology, this idea will gain importance, since both the authors and performers themselves, who risk being replaced by the machine, and their audience are interested in this. The author suggests the creation of a copyright institution that would legally limit the possibility of copying a unique creative style using artificial intelligence technology.

Keywords: Artificial intelligence, Copyright, Creative style, Author, Performer, Creative activity, Quasi-work

Введение. Особую роль в преобразовании нашей жизни играют так называемые «сквозные» технологии, под которыми понимают ключевые научно-технические направления, развитие которых позволит обеспечить радикальное изменение ситуации на существующих рынках технологий, продуктов и услуг [3]. Одной из таких технологий, несомненно, является технология имитации мыслительной деятельности или искусственный интеллект (далее – ИИ). Несмотря на то, что внедрение интеллектуальных систем еще не так глобально, как, например, распространение сети Интернет, тем не менее уже очевидно, что развитие данной технологии будет являться неременным требованием для роста экономики государства и уровня жизни населения. Понимание значимости этой технологии находит отражение в Указе Президента РФ от 10.10.2019 № 490. Этот документ определяет ИИ как технологическое решение, которое способно имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека [2]. Имитация когнитивных функций человека подразумевает способности к запоминанию и анализу новой информации, и, как следствие, приобретению новых знаний. Таким образом, компьютерные системы, наделенные такими возможностями, являются самообучаемыми. Технологии такого уровня, несомненно, будут иметь влияние и изменять социальную, экономическую, культурную и политическую сферы общества.

Сейчас мало кого удивит использование ИИ в том числе и для имитации творческого труда человека. Среди известнейших примеров продажа картины, написанной нейросетью под названием «Портрет Эдмонд Беллами» [9. С. 120–132]. Картина была создана ИИ на основе анализа 15 000 картин, написанных в период с XIV до XX в. Это был первый случай, когда вместе с картинами, написанными людьми, объектом продажи стала картина, созданная машиной. Пожалуй, это стало своеобразной точкой отсчета для признания нейросетевого творчества равным по уровню человеческому творчеству.

Программа на основе ИИ способна с помощью анализа большого количества данных выдавать условно новый результат интеллектуальной деятельности. Поскольку творческий характер процесса создания произведения здесь вызывает вопросы, используем для наименования этого результата концепт «квази-произведение». Стоит ли говорить, что подобного рода результаты достигаются не худож-

никами, музыкантами или поэтами, а программистами. Необходимо подчеркнуть, что программа способна в том числе создавать квази-произведения по заранее установленным параметрам и на основе анализа определенной оператором программы информации. Это дает возможность создавать «новые» произведения, заранее подогнанные под определенный необходимый результат. Таким образом, для энтузиастов открывается простор создания квази-произведений, на основе творческих результатов их кумиров. Здесь в качестве примера стоит отметить проект «Lost Tapes of the 27 Club» организации Over the Bridge [10]. Сотрудники организации использовали программу на основе ИИ, которая создает произведение в стиле музыкантов из так называемого «Клуба 27». Цели проекта далеки от коммерции: авторы этой идеи хотят показать, какие произведения могли бы создать умершие музыканты. Подражание творческому почерку определенных авторов явление не новое. Известно, что некоторые писатели используют в художественных целях прием многоязычия, подражая стилю известных писателей. Однако с появлением и развитием ИИ создание произведений «в стиле» определенных авторов становится в некотором роде новым трендом и происходит уже в «промышленных» масштабах. Здесь хотелось бы вспомнить о технологии голограммы, предполагающей создание оптических клонов любых объектов. Эта технология завоевывает популярность в том числе и в сфере шоу-бизнеса. Так, например, голограмма ныне ушедшего из жизни Ронни Джеймса Дио «отправилась» на мировые гастроли несколько лет назад [5. С. 50–52]. Полагаем, нет никаких сложностей в том, чтобы таким образом «воскресить» известных звезд в мире музыки и уже во вполне коммерческих целях отправить их на гастроли с уже «новыми» хитами, написанными в их стиле. Не стоит исключать подобных случаев «клонирования» творческого почерка и в отношении живых корифеев сферы искусства. Важно помнить, что при всем этом, собственно, ничего нового в творческом плане не создается.

Основная часть. Способность ИИ подражать творческому почерку людей, чья профессиональная деятельность связана с творчеством, а также состоявшихся в этой сфере, ставит этих людей в уязвимое положение. В самом деле, зачем договариваться и нанимать известного художника или музыканта если его творческий почерк сможет повторить компьютерная программа. Надо понимать, что этого никто не сможет заметить, кроме, разумеется, самих художников и музыкантов, чей творческий почерк был повторен.

Если нейросеть способна повторить основные особенности творчества известного писателя, художника или музыканта, то речь, на наш взгляд, идет о копировании стиля. Сегодня творческий стиль не является объектом ни авторского, ни смежных прав. Вместе с тем, Н. Г. Валеева отмечала, что именно «своеобразный стиль» копируют подражатели и, следовательно, он подлежит охране [7]. Однако здесь важно отметить, что Н. Г. Валеева рассуждала об исполнениях. Поможет ли концепт «исполнений» отграничить произведения и квази-произведения? Следует начать с того, что включение «исполнений» в объекты права интеллектуальной собственности имеет дискуссионный характер. Несмотря на то, что в соответствии со статьей 1313 Гражданского кодекса РФ [1] (далее – ГК РФ) исполнение предполагает

творческий характер, некоторые авторы высказываются о некорректности этого положения поскольку исполнение не связано с творчеством, а сами «исполнения» не могут быть объектами интеллектуальной собственности [11]. В дополнении к этому, не вполне понятно, что именно охраняется, ведь каждый объект исполнения создается при каждом акте исполнения, а каждый акт исполнения создает новый результат. Это означает, что сознательное копирование какого-либо исполнителя создает новое исполнение [6. С. 50–52]. Отсюда напрашивается вывод, что охраняется сам процесс, который может быть воспроизведен.

Далее, в международных документах, дается характеристика исполнения как интерпретации исполнителем оригинального авторского произведения [4]. Можно ли допустить тезис о том, что ИИ на основе интерпретаций произведений других авторов создает что-то новое? Полагаем, что нет, ведь для интерпретации необходимо воображение и целеполагание, которое у ИИ отсутствует. Кроме того, интерпретация может меняться в зависимости от творческого стиля, который включает в себя различные составляющие: особую манеру интонирования, способ звукоизвлечения, продумывание поведения персонажа и многое другое (отсюда «интерпретация в стиле...»). По нашему мнению, своеобразный стиль творчества является результатом длительной творческой работы человека, и может меняться в течение жизни, по мере изменения личности человека. Иными словами, творческий стиль является разновидностью результатов творческой (интеллектуальной) деятельности. Разумеется, личности у ИИ нет.

Можно ли соотнести категории «исполнение» и «творческий стиль» как родовидовые? На наш взгляд, ответ должен быть отрицательным. Попытка включить творческий стиль в институт «исполнений» вряд ли будет соответствовать ожиданиям всех заинтересованных субъектов. Дело в том, что в число субъектов-исполнителей включаются артисты-исполнители, дирижеры, режиссеры-постановщики спектаклей. Несомненно, что уникальный творческий стиль есть и у писателей, и у художников. При этом речь идет не только о тех людях, которые пишут картины, а о всех тех, кто занимается изобразительным искусством, архитектурой или декоративно-прикладным искусством. Но их произведения исполнить затруднительно (как можно исполнить картину?). Кроме того, напомним, что, на наш взгляд, исполнение предполагает связь с процессом, а творческий стиль предполагает связь с результатом творческой работы, который может быть выражен как в созданном произведении, так и в процессе исполнения произведения.

Итак, способность ИИ создавать «новые» произведения в стиле определенных авторов сделает актуальным вопрос правовой защиты именного уникального творческого стиля, а не процесса исполнения. В контексте заявленной проблематики решением может быть предложение дополнения четвертой части ГК РФ институтом «творческого стиля». Уникальный творческий стиль есть результат не только длительной творческой деятельности, но и способ проявления качеств личности, способ коммуникации с публикой и воздействия на нее. Именно творческий стиль придает произведению автора или исполнению исполнителя такую совокупность особенностей, которая позволяет отличить его творчество от творчества иных лиц. Таким образом, определяющим критерием наличия собственного творческого сти-

ля является его узнаваемость. Критерий узнаваемости не является чем-то новым в праве. Так, одним из критериев пародии является узнаваемость, то есть неизбежная ассоциация у воспринимающего ее лица с оригинальным произведением [8]. Постановка режиссера-постановщика будет являться результатом исполнительской деятельности, если постановку возможно повторно исполнить, и она сохранит узнаваемость для зрителя. Исходя из сказанного, термин «творческий стиль» может пониматься как совокупность специфических и узнаваемых особенностей творческого процесса или творческого результата деятельности лица.

Отдельной работы требует вопрос о том, к каким объектам права интеллектуальной деятельности будет принадлежать творческий стиль. Выскажем тезисно краткие соображения. Являясь результатом интеллектуальной деятельности, вряд ли творческий стиль может быть отнесен к объектам авторских прав. Произведения являются формой выражения стиля и без произведения не может быть стиля. Некорректным было бы включать творческий стиль в результаты исполнительской деятельности, поскольку исполнительская деятельность есть процесс, а творческий стиль есть результат. Если основным критерием творческого стиля, как было отмечено, является его узнаваемость публикой, то, надо полагать, творческий стиль может быть описан. Результаты интеллектуальной деятельности, которые можно описать и при этом индивидуализирующие субъекта или его деятельность, являются средствами индивидуализации. Таким образом, творческий стиль может являться средством индивидуализации автора или исполнителя.

Хотелось бы подчеркнуть, что цель института творческого стиля должна состоять прежде всего в ограничении возможностей копирования творческого стиля при помощи интеллектуальных систем с технологией искусственного интеллекта. Полагаем, такая мера не позволит вводить аудиторию в заблуждение и укрепит положение людей, чьи профессии связаны с творчеством. Предложение не следует трактовать как призыв ввести полный правовой запрет на «копирование» стилей, к которому неизбежно прибегают авторы и исполнители, во время своего творческого становления или же в сугубо художественных целях. Наличие права на творческий стиль в контексте проблематики настоящей статьи подразумевает возможность авторов или исполнителей, чей стиль был использован в целях создания квази-произведений без согласования с ними, прибегнуть к защите этого права, например, путем пресечения действий, нарушающих право, или же требования указания того, чей стиль был использован программой ИИ. В то же время наличие творческого стиля не исключает передачу права его использования в ходе работы программы на основе ИИ.

Заключение. Сложно однозначно прогнозировать, как использование технологии искусственного интеллекта отразится на творческой деятельности людей. С одной стороны, творческие результаты человеческой деятельности могут получить элемент эксклюзивности. Однако, на наш взгляд, сопоставимость результатов работы программы с творческой деятельностью человека, скорее всего приведет к обесцениванию творческого труда человека. Как результат, уменьшение количества творческих специальностей и вытеснение человека из профессиональной творческой среды. В текущих условиях, учитывая возрастающие возможности искусственного

интеллекта, творческий труд человека будет заменяться (или подменяться) работой программ, а способность ИИ копировать творческий стиль известных авторов и исполнителей, ставит под угрозу карьеры известных личностей в творческой сфере. Одним из способов преодоления такого положения дел могло бы быть введение концепта творческого стиля авторов и исполнителей, под которым может пониматься совокупность специфических и узнаваемых особенностей творческого процесса или творческого результата деятельности лица. Совокупность индивидуализирующих стиль особенностей может быть описана и, таким образом, может являться средством индивидуализации творческой деятельности лица. Возможность обладания уникальным творческим стилем следует признать как за авторами, так и за исполнителями. Появление такого нематериального блага и права на него укрепило бы позиции людей, чья профессиональная деятельность предполагает творческий труд, а возможность передачи права использования творческого стиля в целях создания квази-произведений, дополнительно бы мотивировало авторов и исполнителей к созданию своего уникального творческого почерка.

Не в последнюю очередь юридический концепт творческого стиля полезен и для аудитории, которая ожидает от авторов и исполнителей оригинальных творческих результатов, а имитацию и подражание творческим результатам человека со стороны ИИ воспринимает не более как развлечение. Общая актуальность этой проблематики коррелирует в том числе и с целями создания института авторского права. На наш взгляд, одной из целей создания концепта авторских прав являлось стимулирование авторов к созданию новых произведений, обеспечив им правовую защиту результатов их творческого труда к числу которых может быть отнесен и уникальный творческий стиль. Возможность создателя защитить результаты своего труда мотивирует к творческой деятельности, в чем заинтересована и аудитория. Таким образом, полагаем, что вопрос защиты уникального творческого стиля в эпоху нейросетевого искусства имеет право на дальнейшее обсуждение.

Список литературы

1. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_64629/ (дата обращения: 01.09.2022).
2. О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента РФ от 10.10.2019 № 490 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 01.09.2022).
3. Об утверждении Правил предоставления субсидии из федерального бюджета на оказание государственной поддержки центров Национальной технологической инициативы на базе образовательных организаций высшего образования и научных организаций и Положения о проведении конкурсного отбора на предоставление грантов на государственную поддержку центров Национальной технологической инициативы на базе образовательных организаций высшего образования и научных организаций: Постановление Правительства РФ от 16.10.2017

№ 1251 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_280781/ (дата обращения: 01.09.2022).

4. Договор Всемирной организации интеллектуальной собственности по исполнениям и фонограммам (вместе с «Согласованными заявлениями в отношении Договора...»). Подписан 20.12.1996 // Бюллетень международных договоров. – 2016. № 12. – С. 12–22.

5. Гражданское право: учебник: в 2 т. / С. С. Алексеев, О. Г. Алексеева, К. П. Беляев и др.; под ред. Б. М. Гонгало. – 3-е изд., перераб. и доп. Москва: Статут, 2018. – Т. 1. – 528 с.

6. Беляева И. А., Зяблова А. Ю., Штенников В. Н., Штенников И. В. Исполнения в четвертой части ГК РФ // Юрист. – 2008. № 12. – С. 50–52.

7. Быкова Эжена. Голограмма Ронни Джеймса Дио отправится на мировые гастроли // Выпуск от 27.07.2017 // Портал Субкультура. URL: <https://sub-cult.ru/subnews/8472-gologramma-ronni-dzheimsa-dio-mirovye-gastroli> (дата обращения: 03.09.2022).

8. Гаврилов Э. П., Еременко В. И. Комментарий к части четвертой Гражданского кодекса Российской Федерации (постатейный). Москва: Экзамен, 2009. – 973 с.

9. Колосов В. А. Пародия в системе авторского права // Закон. 2013. № 9. С. 120–132.

10. Мироненко Владимир. Созданная искусственным интеллектом картина продана на аукционе за \$ 432 000 // Выпуск от 27.10.2018 // 3DNews: сайт. URL: <https://3dnews.ru/977354/sozdannaya-iskusstvennim-intellektom-kartina-prodana-na-auktsione-za-432-000> (дата обращения: 01.09.2022).

11. Сафронова Виктория. Нейросеть создает песни Nirvana, Эми Уайнхаус и других музыкантов. Проект помогает артистам с психологическими проблемами // Выпуск от 05.04.2021 // Naked Science. сайт. URL: <https://naked-science.ru/article/hi-tech/nejroset-sozdaet-pesni-nirvana> (дата обращения: 01.09.2022).

А. В. Алешина,

кандидат экономических наук, доцент,

Московский государственный университет имени М. В. Ломоносова

А. Л. Булгаков,

кандидат экономических наук,

Московский государственный университет имени М. В. Ломоносова;

доцент, Российский экономический университет

имени Г. В. Плеханова

ФИНАНСОВОЕ МОШЕННИЧЕСТВО И ЦИФРОВЫЕ ТЕХНОЛОГИИ

Аннотация. Финансовые инновации с цифровыми технологиями способствуют сокращению скорости совершения финансовых операций, повышают доступность финансовых услуг, делают получение услуг более комфортным и требующим меньше затрат времени на их оформление. Вместе с тем финансовые цифровые технологии

влекут за собой риски и новые виды мошенничества (например, с использованием токенов), рост количества банкротств финтех-компаний и криптобирж, что принесло их клиентам и инвесторам большие убытки. Регулирование финтеха в настоящее время осуществляется в более льготном режиме, чем регулирование традиционных финансовых институтов: банков, страховых компаний, брокеров и бирж. Появляются «регулятивные песочницы» (Regulatory sandbox), которые устанавливаются финансовыми регуляторами для более легкого входа на рынок финансовых технологий в заранее заданном регуляторном поле. Модели работы «регулятивных песочниц» различаются в разных странах. Требуется разработка таких рамок «регулятивных песочниц», которые бы позволили появляться новым финансовым технологиям, с одной стороны, но, с другой стороны, обеспечивали бы стабильность финансовой системы в целом и защиту прав инвесторов в частности.

Ключевые слова: финтех, децентрализованные финансы, токены, регулятивные песочницы, финансовое мошенничество, финансовое регулирование

FINANCIAL FRAUD AND DIGITAL TECHNOLOGIES

Abstract. Financial innovations, digital technologies, on the one hand, help to reduce the speed of financial transactions, increase the availability of financial services, make receiving services more comfortable and require less time to process them. On the other hand, new financial digital technologies entail new risks and new types of fraud. In recent years, the number of token scams has increased dramatically. The number of bankruptcies of fintech companies and crypto-exchanges has increased, which brought them big losses to their clients and investors. Fintech regulation is currently carried out in a more preferential regime than the regulation of traditional financial institutions: banks, insurance companies, brokers and exchanges. Regulatory sandboxes are emerging, which are set up by financial regulators to facilitate entry into the fintech market within a predetermined regulatory field. Regulatory sandbox models vary from country to country. It is necessary to develop such a framework of «regulatory sandboxes» that would allow the emergence of new financial technologies, on the one hand, but, on the other hand, would ensure the stability of the financial system in general and the protection of investors' rights in particular.

Keywords: FinTech, decentralized finance (DeFi), tokens, regulatory sandboxes, financial fraud, financial regulation

Введение. Статистика последних лет демонстрирует большое количество случаев финансового мошенничества с использованием цифровых финансовых технологий (см. рис. 1, 2, 3), в том числе токенов, крипто-бирж, финтех-компаний, цифровых финансовых активов, а также с помощью методов социальной инженерии с использованием цифровых технологий.

Мошенничества с предодобренными кредитами и средствами социальной инженерии. Вопросы мошенничества с кредитами затрагивают не только те ситуации, когда заемщик получает в банке кредит на основании ложных документов о своих доходах и месте работы.

В последние годы участились количества случаев мошенничества при кредитовании с использованием цифровых технологий и методов социальной инженерии. Мошенники получают информацию из различных источников: интернет-магазинов, различных сайтов, через которые проходила оплата заказов, сайтов, которые специально созданы для сбора подобной информации, маркетинговых опросов. Для совершения мошенничества обычно достаточно получить номер телефона, ФИО клиента банка, название банка, в котором у клиента есть счет. В результате клиент банка получает звонок от мошенников, которые представляются сотрудниками кредитного отдела банка или службы безопасности банка, в котором у клиента есть счет. Они сообщают о попытке мошенников оформить кредит от имени клиента и для предотвращения хищения средств в виде оформленного кредита, который прямо сейчас оформляют мошенники, «представители банка» предлагают клиенту установить специальное программное обеспечение, чтобы защитить персональные данные и отменить заявку на кредит. Эти программы или давали мошенникам удаленный доступ к компьютеру или телефону клиента банка, где мошенники уже самостоятельно могли перевести деньги клиента на свои счета.

Или мошенники предлагали клиенту самому перевести деньги на «специальный счет», чтобы «уберечь» деньги от мошенников, но именно этот счет и оказывался счетом мошенников [кейсы 4, 5, 6]. Речь идет о мошеннических операциях не менее чем на 1 млн. рублей по каждому случаю. По мнению банковских экспертов, речь идет о нескольких тысячах таких случаев в год [2]. Согласно статистике Центрального банка РФ существует большое количество банковских операций, которые проведены без согласия клиентов банка (физических и юридических лиц), которые выросли практически на 33,8% за последний год (с 773 тыс. ед. операций в 2020 году до 1035 тыс. ед. операций в 2021 году) [1. С. 68; 6]. При этом общий объем ущерба от таких операций также вырос на 38,8% (с 9783 млн руб. в 2020 году до 1358 млн. руб. в 2021 году).

При этом объем возвращенных средств пострадавшим клиентам составляет согласно статистике Центрального банка РФ не более 5-7% в 2021-2022 годах [7].

Такая ситуация требует принятия поправок в законодательство, которые позволят более эффективно работать связке правоохранительных органов, Центрального Банка России и коммерческих банков и снизить количество времени, которое требуется для блокирования подозрительных финансовых операций. Необходимо установить в нормативных актах срок блокирования таких операций не более чем сутки с момента появления информации о подозрительной операции по жалобе клиента-отправителя средств. Далее, если клиент-получатель средств готов подтвердить законность получения денег, он должен будет лично явиться в отделение банка с документами, подтверждающими его личность и при личной явке должны быть выяснены причины блокировки средств и разрешен спор между отправителем и получателем средств. Если спор сохраняется, то деньги далее не должны уходить и спор должен разрешаться в рамках установленных в законодательстве процедур, в том числе через суд. Такой механизм оперативной блокировки средств по жалобе отправителя позволит снизить количество случаев мошенничества с использованием финансовых технологий, предотвратит кражу денег и повысит процент возврата украденных с помощью финансовых технологий средств.

Финансовые мошенничества и цифровые финансовые активы, токены и криптовалюта. Появление цифровых финансовых активов, токенов и криптовалюты увеличило, с одной стороны, скорость совершения финансовых операций, снизило издержки на совершение сделок, но, с другой стороны, увеличило возможность для совершения финансовых мошенничеств [1. С. 68].

В последние годы резко увеличилось количество мошенничеств с использованием токенов. По статистике Лаборатории Солидус (Solidus Labs) [10] за два года с сентября 2020 года по 1 декабря 2022 года количество мошенничеств с помощью токенов составило более 200 тыс инцидентов (см. рис. 1). Это практически 15 мошеннических проектов в час [10]. По информации Лаборатории Солидус наиболее частая схема мошенничества с токенами называется «rug pull», когда мошенники выпускают токены, распродают их инвесторам, которые рассчитывают быстро на токенах заработать, и скрываются с полученными денежными средствами.

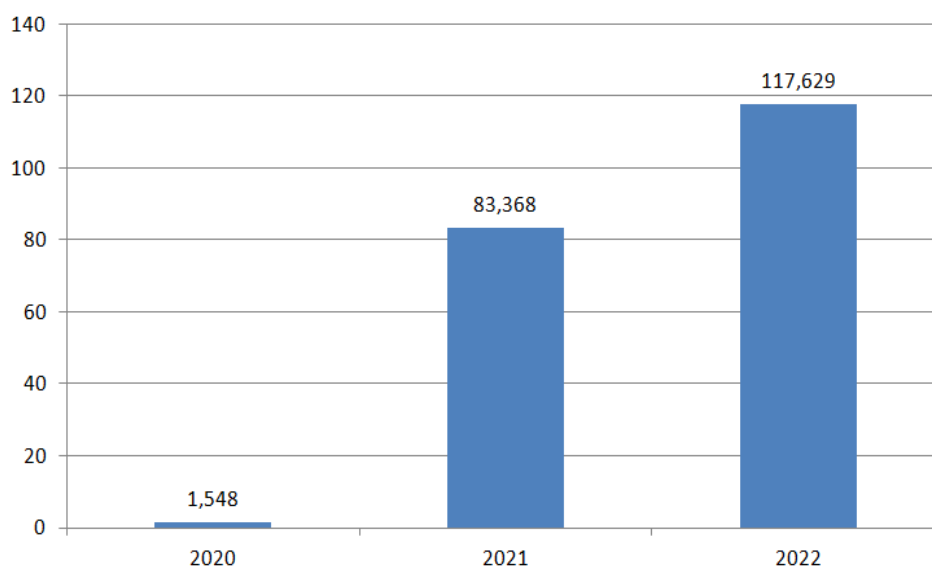


Рис. 1 Мошеннические токены, появившиеся за год в тыс. единиц [10. С. 4]

По статистике Solidus Labs мошенники используют фиктивные токены, криптовалютные биржи для осуществления хищения денежных средств клиентов и инвесторов. Сумма похищенных средств по оценкам составляет 11 млрд. долларов США, при этом основные хищения происходят с использованием криптовалютных бирж пяти юрисдикций: США, Сейшельские острова, Багамы, Нидерланды и Гонконг (см. рис. 2).

За последние годы существует большое количество случаев инцидентов с мошенничеством, связанным с финансовыми технологиями, в том числе мошеннические токены, банкротство криптобирж, банкротство финтех-компаний. И объем потерянных средств инвесторов постоянно растет (см. рис. 3).

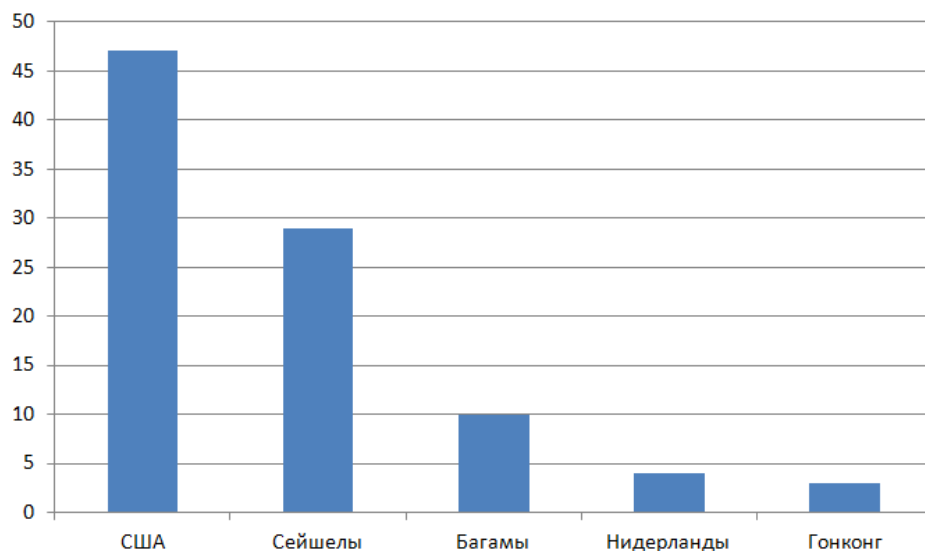


Рис. 2. Централизованные биржи, через которые происходят мошеннические операции с токенами, по юрисдикциям (5 топ юрисдикций), млрд долларов США украденных средств инвесторов, пострадавших от мошеннических токенов [10. С. 4]

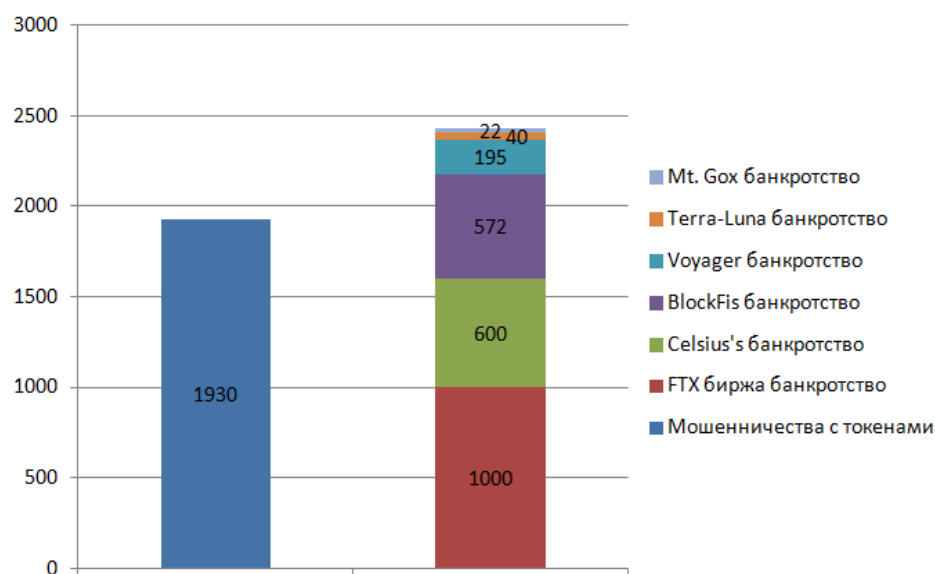


Рис. 3. Сумма убытков криптоинвесторов от инцидентов с финтех-компаниями, в миллионах долларов США [10. С. 5]

Рост случаев банкротств финтех-компаний, в первую очередь от мошеннических действий руководства этих компаний, вызывает запросы со стороны инвесторов, как физических лиц, так и инвестиционных компаний, о введении хотя бы минимально необходимого объема регулирования финтех-компаний.

Регулирование финтеха: регуляторные песочницы и финансовые мошенничества. Регулирование финтеха в настоящее время осуществляется в более льготном режиме, чем регулирование традиционных финансовых институтов: банков, страховых компаний, брокеров и бирж. В то время как традиционные финансовые институты должны сдавать достаточно объемную отчетность в регулирующие органы (в Центральный банк, в Министерство финансов, в комиссии по ценным бумагам (в зависимости от того, какой орган регулирует финансовые институты в данной стране)), соблюдать достаточно высокие требования к собственному капиталу, а также достаточно высокие нормативы своей деятельности, то финтех-компании во многих странах подвергаются более льготному регулированию.

В частности, существует такое понятие как регуляторная (регулятивная) песочница (Regulatory sandbox). Регулятивная песочница представляет собой тестовую зону, которая установлена на ограниченный срок и охватывает узкую область работы инновационных технологий, которые тестируются для работы в реальной жизни, в рамках которой установлено минимальное регулирование для начинающих финансовых технологий и стартапов или оно полностью отсутствует [13]. Введение такого механизма как регулятивные песочницы направлено на создание льготного режима для начинающих финансовых технологий, с которыми заранее непонятно: будут ли они удачными, если их подвергать классическому регулированию финансовых институтов. То есть существует высокая вероятность, что при введении традиционного регулирования финансовых институтов в отношении финтех стартапов эти организации просто не смогут реализовать свои технологии и протестировать свою стратегию.

Центральный банк России использует термин регулятивная песочница, под которым понимает «механизм для пилотирования, моделирования процессов новых финансовых сервисов и технологий в изолированной среде, требующих изменения правового регулирования» [9]. Центральный банк России согласился внедрить в российскую практику такой механизм для достижения следующих целей: запуска инновационных финансовых сервисов без риска нарушения законодательства РФ, выявления и проверки рисков финтех-сервисов и предложение подходов к их снижению, а также проверки целесообразности работы финтех-сервисов.

Центральный банк России установил правила работы регулятивной песочницы, которые заключаются в том, что любая компания, которая хочет протестировать новый финтех-проект, может подать заявку в ЦБ РФ о желании провести такое тестирование. Центральный Банк России оценивает целесообразность такого решения, проводит пилотирование проекта и принимает решение о целесообразности внедрения проекта, после чего ЦБ РФ утверждает дорожную карту по созданию правовых условий для внедрения сервиса [9]. Первый проект, который был реализован в рамках регулятивной песочницы в 2019 году и был согласован Центральным Банком России, это сервис, позволяющий дистанционно управлять полномочиями по счетам корпоративных клиентов на совершение операций в отделениях банков [8]. В том же 2019 году получил одобрение ЦБ РФ другой сервис, который позволял банкам оценивать кредитоспособность потенциальных заемщиков, используя информацию от операторов фискальных данных о выручке предпринимателей, сведения об их операциях по расчетному счету и данные их контрагентов [7].

Наиболее прорывным инструментом, согласованным Центральным банком России в рамках регулятивной песочницы, был проект ПАО «ГМК «Норильский никель» по созданию блокчейн-платформы для выпуска и оборота цифровых прав, которая позволяет оцифровать (токенизировать) товары, услуги, ценные бумаги и другие активы. Данная площадка позволит осуществлять выпуск гибридных токенов, которые обеспечены разными активами, в том числе сырьем [3].

Создание регулятивных песочниц дает одновременно плюсы и минусы для финансового сектора. С одной стороны, такой либеральный подход к регулированию новых финтех-компаний дает возможность появиться и развиваться компаниям в области инновационных финансовых решений, которые в условиях жесткого регулирования просто не смогли бы появиться. С другой стороны, такой льготный подход к регулированию позволяет появиться и получить расширенное развитие мошенническим компаниям. Ярким примером являются кейсы с финтех-компаниями (банками) Wirecard и Greensill. Регулирующие финансовые органы в Германии и в других странах позволили банкам, контролируемым Wirecard и Greensill, совершать рискованные финансовые операции, осуществлять злоупотребления, которые повлекли за собой высокие убытки инвесторов.

Wirecard осуществляла займы в пользу своих материнских компаний на нерыночной основе, осуществляла мошеннические переводы средств в подконтрольные компании. Greensill банк предоставлял льготные кредиты родительской финтех компании. Регуляторы не предприняли своевременных мер в отношении банков Wirecard и Greensill, потому что не осуществлялся консолидированный надзор за группой связанных компаний, не осуществлялся надзор за деятельностью их международных структур, которые создали оба этих банка. Крах этих финтех-банков нанес существенный ущерб их инвесторам, кредиторам, регуляторам и другим заинтересованным сторонам.

Банкротство Wirecard и Greensill наглядно демонстрирует риски, которые могут за собой влечь регулятивные льготы, предоставляемые финтех-компаниям в области банковских услуг в условиях отсутствия надлежащего пруденциального надзора, который обычно применяется к классическим коммерческим банкам.

Аналогичная точка зрения высказывается в работе Артура Э. Уилмарта «Wirecard and Greensill Scandals Confirm Dangers of Mixing Banking and Commerce» [14]. Уилмарт говорит о рисках того, что многие новые финтех-банки принадлежат или контролируются коммерческими предприятиями. Связи между коммерческими фирмами и банками, занимающимися финансовыми технологиями, вызывают новые опасения по поводу опасностей смешения банковского дела и коммерции. Скандалы с Wirecard и Greensill Capital (Greensill) показывают потенциальный масштаб этих опасностей. В последние годы в США Федеральная корпорация страхования депозитов (FDIC) и Управление валютного контролера (ОСС) поощряют коммерческие предприятия приобретать финтех-банки. В том числе FDIC разрешил коммерческим фирмам приобретать банки, застрахованные FDIC, полагаясь на лазейку в Законе о банковских холдинговых компаниях (Bank Holding Company Act, BHC Act). ОСС стремится создать недепозитные национальные финтех-банки, которыми коммерческие фирмы могли бы владеть в соответствии с отдельным исключением в Законе

ВНС. Инициативы FDIC и OCC, по мнению Уилмарта, подрывают – и потенциально могут разрушить – давнюю политику ВНС Act по разделению банковского дела и торговли.

Дирк Цетше и др. в работе «Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation» утверждает, что необходимо отказаться от идеи излишне либерального регулирования финтех-компаний и банков и установить новый подход к регулированию, который будет включать в себя сбалансированные цели регулирования, который он назвал «разумное регулирование» (Smart Regulation) [15]. Цетше подчеркивает, что произошло изменение в подходах к регулированию финансового сектора. Если до кризиса 2008 года господствовала концепция дерегулирования финансовых институтов и финансовых инструментов, то после кризиса маятник качнулся в обратную сторону и произошло ужесточение регулирования финансовых институтов.

Такое ужесточение регулирования традиционных финансовых институтов, и, в первую очередь, банков, повлекло за собой повышение доходности финтех-компаний, которые могли предоставлять аналогичные банковским услуги, но при этом не подвергались такому жесткому регулированию, которому подвергались классические банки и которое требует существенных затрат для соответствия регуляторным требованиям.

Цетше в своей работе проанализировал подходы к регулированию финтеха в разных странах, начиная от полного бездействия регулятора, осторожной вседозволенности (в каждом конкретном случае или с помощью специальных уставов и актов), структурированного экспериментализма (например, песочницы или пилотирования) и разработки специального нового подхода к регулированию финтеха [15].

Цетше предлагает соблюдать ряд требований при разработке подходов к регулированию финтех-компаний.

– Во-первых, он предлагает оценивать величину риска того, что банкротство данной финтех-компании может повлиять на стабильность всей финансовой системы. В случае высокого риска воздействия на стабильность финансовой системы регулирование финтех-компаний должно быть все-таки осуществлено.

– Во-вторых, фактор, который должен оцениваться – это прозрачность рынка, а также степень защиты интересов клиентов, потребителей, контрагентов и других участников финансовой системы.

– В-третьих, автор предлагает оценивать необходимость наличия регулятивной песочницы, так как если технология, услуга или вид деятельности уже должным образом регулируются существующим законодательством и нормативными актами, то отсутствует необходимость в предоставлении регулятивной льготы.

– В-четвертых, он предлагает регулятору при установлении льготных регуляторных мер, все-таки требовать адекватной подготовки финтех-компаний для вхождения в такие льготные меры, в том числе необходимость вхождения в стадию разработки нового финтех-решения, понимание законов и нормативных актов, которые регулируют данную сферу, а также наличие достаточного механизма у финтех-компаний по управлению возможными рисками [15].

В настоящее время разброс юридических решений в сфере предоставления льготных регуляторных режимов в разных странах достаточно существенный. Если

в Гонконге допуск на рынок разрешен только для зарегистрированных (авторизованных) фирм (Fintech Supervisory Sandbox (FSS)) [12], то в Сингапуре [11] новым финтех-компаниям предоставляют ограниченную лицензию на деятельность.

Fintech Supervisory Sandbox (FSS), запущенный НКМА (Hong Kong Monetary Authority) в сентябре 2016 года, позволяет банкам и их партнерским технологическим фирмам (финтех-компаниям) проводить пилотные испытания своих финтех-инициатив с участием ограниченного числа участвующих клиентов без необходимости достижения полного соответствия надзорным требованиям НКМА. Это соглашение позволяет банкам и технологическим компаниям собирать данные и отзывы пользователей, чтобы они могли вносить усовершенствования в свои новые инициативы, тем самым ускоряя запуск новых технологических продуктов и снижая стоимость разработки. [12]

В дополнение к функции пилотных испытаний, предлагаемой в Гонконге правилами FSS 2.0, правила FSS 3.0 облегчают приемлемые пробные проекты исследований и разработок (R&D) для подачи заявок на получение финансовой поддержки в размере не более 1 млн. гонконгских долларов в рамках программы испытаний в государственном секторе Комиссии по инновациям и технологиям (ITC) (PSTS) [12].

В то же время в Сингапуре регулятор установил, что финансовые институты уже в настоящее время могут свободно запускать новые финансовые продукты, услуги или процессы («финансовые услуги») без предварительного получения разрешения MAS [11], при условии, что они осуществляют должную осмотрительность и в их деятельности отсутствуют нарушения правовых и нормативных требований. Однако, регулятор подчеркивает, что новые финансовые услуги, использующие финтех, становятся все более сложными, и может возникнуть неопределенность в отношении того, соответствует ли инновация нормативным требованиям. Для того чтобы позволить финансовым институтам протестировать новые финансовые технологии без риска нарушения законодательства, регулятор в Сингапуре позволяет подать любой заинтересованной фирме заявку на участие в регулятивной песочнице для экспериментов с инновационными финансовыми услугами в производственную среду, но в пределах четко определенной территории действия и заранее установленной продолжительности времени. При этом должны соблюдаться соответствующие меры предосторожности для сдерживания последствий банкротства финтех-компаний и поддержания общей безопасности и надежности финансовой системы.

Однако существует и противоположный подход к регулированию финтех-компаний. Такие страны, как Германия, США, Франция и Люксембург не приняли практику регулятивных песочниц. По сути их льготу можно назвать «льготой бездействия». Регулирующие органы этих стран реагируют на появившуюся финансовую технологию, новый финансовый продукт последующим вмешательством, если посчитают, что такая деятельность нарушает существующее законодательство или интересы инвесторов. На начало деятельности таких компаний регуляторы этих стран обычно реагируют молчанием, и только в последующем, если они считают, что происходит нарушение закона, они вмешиваются и требуют соблюдения общих норм регулирования для всех финансовых организаций.

Наглядным примером является кейс с токенами компании Телеграм (Telegram), когда комиссия по ценным бумагам США (SEC) в 2020 году подала иск в суд к компании Telegram, которая незадолго до этого провела мероприятия по размещению токенов криптовалюты GRAM. Комиссия посчитала, что токены криптовалюты GRAM обладают признаками ценной бумаги и требуют предварительного получения разрешения на их размещение в Комиссии. В связи с тем, что компания Telegram осуществила размещение токенов не получая разрешение SEC, как того требует закон о ценных бумагах США 1933 года, комиссия обратилась в суд с просьбой запретить размещение этих токенов в связи с отсутствием регистрации в SEC. В рамках первичного размещения в 2018-2020 годах Telegram привлек около 1,7 млрд. долларов США инвестиций от частных инвесторов, банков и хедж-фондов. 24 марта 2020 года судья окружного суда Нью-Йорка Кевин Кастел предварительно признал токены криптовалюты GRAM ценной бумагой, что означало запрет на передачу токенов инвесторам. 12 мая 2020 года компания Telegram прекратила дальнейшую разработку токенов и приняла решение об отзыве апелляции на решение суда и прекращении дальнейших судебных споров.

Такой подход к регулированию финтех-проектов в США, с одной стороны, предоставляет возможность инновационным фирмам протестировать новый финтех-продукт и оценить его эффективность, но, с другой стороны, он лишает финтех-компании определенности в будущем развитии событий, когда уже подготовленный проект может быть заблокирован на конечной стадии реализации в связи с позицией регулятора о необходимости соблюдения общих для всех финансовых компаний и банков регулятивных мер.

Наличие предсказуемости в поведении регулятора и возможность заранее оценивать регуляторные риски является важным элементом создания инновационной площадки в стране для развития финтех-компаний. Поэтому действия российского Центрального Банка, который установил понятие регулятивной песочницы и заранее определил границы, в рамках которых будет действовать льготное регулирование для финтех-компаний, воспринимается участниками рынка как более предпочтительное с точки зрения предсказуемости регулятора в своих действиях и с точки зрения пределов регулирования финтех-компаний.

Список литературы

1. Алешина А. В., Булгаков А. Л., Котов А. В., Трошков О. Г. Развитие методов противодействия мошенничеству в банковской и финансовой сферах в условиях цифровизации // Финансовые рынки и банки. № 10. 2022. С. 68–74. URL: http://www.finmarketbank.ru/archive/?ELEMENT_ID=36542 (дата обращения: 06.09.2022).
2. Банки предупредили о всплеске хищений предварительно одобренных кредитов. Мошенники получают удаленный доступ к телефонам жертв или убеждают их самих перевести деньги. URL: <https://www.rbc.ru/finances/31/10/2020/5f9afd879a79470cfa72e8e7> (дата обращения: 08.09.2022).
3. Выпуск цифровых прав на блокчейн-платформе: пилотный проект в регулятивной «песочнице» // Портал Центрального Банка России от 17.02.2020. URL: <https://cbr.ru/press/event/?id=6387#highlight=песочнице> (дата обращения: 20.09.2022).

4. Кейс 1 по мошенничеству с кредитом в Альфа-банке. URL: <https://www.banki.ru/services/responses/bank/response/10430167/> (дата обращения: 20.09.2022).
5. Кейс 2 по мошенничеству с кредитом в Альфа-банке. URL: https://www.banki.ru/forum/?PAGE_NAME=read&FID=61&TID=380400 (дата обращения: 20.09.2022).
6. Кейс 3 по мошенничеству с кредитом в Альфа-банке. URL: https://www.banki.ru/forum/?PAGE_NAME=message&FID=61&TID=380400&MID=8279063#message8279063 (дата обращения: 20.09.2022).
7. Новые сервисы для кредитования малого и среднего бизнеса из регулятивной «песочницы»: портал Центрального Банка России от 22.08.2019. URL: <https://cbr.ru/press/event/?id=2818#highlight=песочницы> (дата обращения: 20.09.2022).
6. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году: портал Центрального Банка России от 11.04.2022. URL: https://cbr.ru/analytics/ib/operations_survey_2021/#1 (дата обращения: 20.09.2022).
7. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за 2 квартал 2022 года // [Электронный ресурс]. – Портал ЦБ РФ от 25 августа 2022 года // URL: https://cbr.ru/analytics/ib/review_2q_2022/ (дата обращения: 20.09.2022).
8. Первый проект из регулятивной «песочницы» Банка России получил юридическую основу: портал Центрального Банка России от 08.02.2019. URL: <https://cbr.ru/press/event/?id=2404#highlight=песочницы%7Спесочнице> (дата обращения: 20.09.2022).
9. Регулятивная «песочница»: портал Центрального банка России. URL: https://cbr.ru/fintech/regulatory_sandbox/ (дата обращения: 20.09.2022).
10. Everything you need to know about rug pulls: Аналитический отчет: портал Лаборатории Солидус (Solidus Labs). URL: https://www.soliduslabs.com/reports/rug-pull-report?utm_source=twitter&utm_medium=twitter&utm_campaign=rug_pull_report (дата обращения: 20.09.2022).
11. Fintech regulatory sandbox guidelines // Monetary authority of Singapore. Guidelines, at 15: портал Монетарного управления Сингапура. URL: <https://www.mas.gov.sg/-/media/mas-media-library/development/regulatory-sandbox/sandbox/fintech-regulatory-sandbox-guidelines-jan-2022.pdf> (дата обращения: 20.09.2022).
12. Fintech Supervisory Sandbox (FSS): портал Монетарного управления Гонконга (Hong Kong Monetary Authority). URL: <https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/fintech-supervisory-sandbox-fss/> (дата обращения: 20.09.2022).
13. Making space for innovation. The handbook for regulatory sandboxes: Федеральное министерство экономических отношений и энергетики Германии. Июль 2019. URL: https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/handbook-regulatory-sandboxes.pdf?__blob=publicationFile&v=2 (дата обращения: 20.09.2022).
14. Wilmarth, Arthur E., Wirecard and Greensill Scandals Confirm Dangers of Mixing Banking and Commerce (May 1, 2021). 40 Banking & Financial Services Policy Report No. 5 (May 2021) , GWU Legal Studies Research Paper No. 2021-23, GWU Law School Public Law Research Paper No. 2021-23, Available at SSRN: <https://ssrn.com/abstract=3849567> (дата обращения: 20.09.2022).

15. Zetzsche, Dirk Andreas and Buckley, Ross P. and Arner, Douglas W. and Barberis, Janos Nathan, *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation* (August 14, 2017). 23 *Fordham Journal of Corporate and Financial Law* 31-103 (2017), European Banking Institute Working Paper Series 2017 - No. 11, University of Luxembourg Law Working Paper No. 006/2017, University of Hong Kong Faculty of Law Research Paper No. 2017/019, UNSW Law Research Paper No. 17-71, Center for Business and Corporate Law (CBC) Working Paper Series 001/2017, Available at SSRN: <https://ssrn.com/abstract=3018534> or <http://dx.doi.org/10.2139/ssrn.3018534> (дата обращения: 20.09.2022).

М. В. Анюрова,

студент,

Тульский государственный университет

БЛОКЧЕЙН КАК ИЗБИРАТЕЛЬНАЯ ТЕХНОЛОГИЯ: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Аннотация. Рассматривается проблема влияния цифровых технологий на реализацию конституционных прав и свобод человека и гражданина, в частности, на избирательное право. Исследуется правовое регулирование и организационные особенности эксперимента по дистанционному электронному голосованию, а также технологическая специфика действия технологии блокчейн. Отмечается, что мировой опыт проведения процедуры дистанционного электронного голосования позволит преодолеть недостатки данной электоральной процедуры. Высказывается положение о том, что актуализация законодательства в сфере действия избирательного блокчейна позволит расширить его применение.

Ключевые слова: право, дистанционное электронное голосование, блокчейн, выборы, цифровизация, избирательный эксперимент

BLOCKCHAIN AS A SELECTIVE TECHNOLOGY: ADVANTAGES AND DISADVANTAGES

Abstract. The problem of the influence of digital technologies on the realization of constitutional rights and freedoms of man and citizen, in particular, on the right to vote, is considered. The legal regulation and organizational features of the remote electronic voting experiment as well as the technological specifics of the blockchain technology are being investigated. It is noted that the world experience of conducting a similar procedure will allow overcoming the shortcomings of this electoral procedure. It is stated that the updating of legislation in the scope of the electoral blockchain will expand its application.

Keywords: Law, Remote electronic voting, Blockchain, Elections, Digitalization, Electoral experiment

Современный этап общественного развития связан с широким распространением информационных технологий. Проблема цифровизации окружающей действительности становится предметом исследований политологов, социологов,

юристов. Значительное место в науке занимают вопросы внедрения информационных достижений в деятельность органов государственной власти, обеспечение защиты права на интеллектуальную собственность, защита персональных данных и другие.

Информационные процессы находят практическое отражение в правовых явлениях: в частности, они оказывают влияние на реализацию конституционных прав и свобод человека и гражданина. Право избирать и быть избранным, закрепленное в ст. 32 Конституции Российской Федерации [1], было конкретизировано в связи с принятием Федерального закона от 23.05.2020 № 154-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», где вводится понятие «дистанционное электронное голосование», под которым понимается голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием специального программного обеспечения [3].

В этой связи особую актуальность приобретает проблема применения технологии блокчейн в избирательном процессе. Ее название произошло от английских слов block («блок») и chain («цепочка»), поэтому можно сделать вывод, что технология предполагает хранение информации в виде цепочки блоков. Действительно, суть блокчейна состоит в распределении данных по последовательно пронумерованным блокам, поэтому при внесении изменений обязательно составляется запись о таких действиях, которая дублируется во все копии, при этом не допускается удаление данных. Таким образом обеспечивается безопасность и сохранность информации [5. С. 4].

Отметим, что идея применения блокчейна в жизни общества отнюдь не нова и нашла практическое выражение в различных сферах. В частности, в банковском секторе она обеспечивает фиксацию полученной информации обо всех совершенных пользователями операциях с криптовалютой.

В рамках нашего исследования будет рассмотрен эксперимент дистанционного электронного голосования, проведенный в Москве в 2019 г. при выборе депутатов Московской городской Думы седьмого созыва. Нормативную основу данной процедуры составили Закон города Москвы «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» [4] и Федеральный закон от 29 мая 2019 г. № 103-ФЗ «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» [2].

Для проведения эксперимента было образовано три цифровых избирательных округа. При этом основанием для включения территории в избирательный округ стало желание самих избирателей: по итогам голосования на портале «Активный гражданин» в состав соответствующих округов вошли территории, набравшие наибольшее число голосов. После этого Московская городская избирательная комиссия утвердила список участковых и территориальных избирательных комиссий, ответственных за проведение дистанционного электронного голосования.

Для участия избирателя в данном эксперименте необходимо было подать электронное заявление через Московский портал государственных и муниципальных

услуг не ранее чем за 45 и не позднее чем за 3 дня до дня голосования. Такой срок был предусмотрен для возможности тщательной проверки информации о включении избирателя в список по соответствующему избирательному участку. Усиленный контроль был обусловлен необходимостью исключить риски повторного голосования, что стало бы нарушением принципа равного избирательного права [6. С. 56].

Непосредственно дистанционное электронное голосование проводилось в то же время, что и голосование на обычных избирательных участках – 8 сентября. Сначала избиратель вводил логин и пароль для входа в личный кабинет на портале мэра и Правительства Москвы, а затем для получения доступа к электронному бюллетеню вводил код, направленный по СМС на его номер телефона, и после этого мог проголосовать.

Именно в процессе передачи персональных данных избирателей и их голосов была использована технология блокчейн. Ее применение можно представить в виде следующих стадий [8]:

1) формирование частей ключа расшифрования, которые разделяются в порядке, установленном территориальной избирательной комиссией по дистанционному электронному голосованию. При этой процедуре могут присутствовать члены комиссии, наблюдатели и представители СМИ;

2) зашифровка результатов голосования, в процессе которой информация разделяется на блоки и анонимизируется, а затем передается в программно-технический комплекс (ПТК ДЭГ). Каждый ключ хранится на отдельном внешнем носителе, который запечатывается в конверт и передается лицу, определенному председателем ТИК ДЭГ;

3) после окончания времени голосования председатель ТИК запускает процедуру расшифрования результатов волеизъявления.

По окончании периода подачи голосов члены участковых избирательных комиссий распечатывали протокол, сформированный по итогам голосования, подписывали его и направляли в вышестоящие комиссии по стандартной процедуре. Явка среди электронных избирателей составила 87,37 % [7. С. 155]. В целом новый способ голосования обеспечил прирост явки в 0,7 % по сравнению с выборами в 2014 г.

Обобщая анализ федерального законодательства, а также данных статистики, можно сделать вывод, что технология блокчейн представляется эффективной формой реализации дистанционного электронного голосования. Преимущества данной электоральной технологии видятся в следующем: блокчейн обладает прозрачностью и анонимностью, так как все операции совершаются открыто, каждый может ознакомиться с историей совершаемых транзакций, но не сможет получить информацию об отправителе и получателе; внесение изменений в части бюллетеней возможно только одобрением большинства участников сети, что обеспечивает защиту системы от взлома; блокчейн обеспечивает тайну волеизъявления и сохранность голосов избирателей, так как расшифрование результатов волеизъявления возможно только при соединении ключевой пары – открытого и закрытого ключей, которые хранятся на защищенных носителях.

Вместе с тем нельзя не упомянуть о недостатках, присущих данной технологии, которые связаны с отсутствием единой нормативной базы, регулирующей действие

блокчейна; его совмещение с другими сервисами (портал mos.ru, анонимайзер), что создает определенные риски сбоя системы из-за необходимости скрещивать разные по содержанию технологии; невозможность изменить голос, в случае если избиратель случайно поставил галочку в электронном бюллетене.

На наш взгляд, для преодоления указанных выше недостатков имеет смысл обратиться к мировой правовой практике: например, использовать опыт Эстонии, Швейцарии, Франции. Несмотря на различия в результатах электронных выборов в этих странах, у них существуют общие технологические черты в организации дистанционного электронного голосования. В частности, можно сказать, что все указанные выше страны используют специфические способы идентификации личности избирателя (ID-карта гражданина с двойным ПИН-кодом, одноразовая карта для голосования с секретным кодом, смарт-карта), которые обеспечивают защиту персональных данных избирателя, исключают риски, связанные с возможностью утечки данных, позволяют менять голос в течение определенного времени. Представляется, что такие организационные особенности могут быть полезны при разработке решений по устранению недостатков, проявившихся при проведении эксперимента в 2019 г.

Таким образом, технология блокчейн в избирательном процессе на сегодняшний день является эффективной формой реализации дистанционного электронного голосования и действенным способом обеспечения безопасности персональных данных избирателей, а также принципа тайного голосования. Несмотря на явные риски и недостатки данной системы, ее положительное влияние на избирательный процесс очевидно. Представляется, что решение задач по актуализации и обновлению законодательства в сфере использования блокчейна в электоральной сфере, по обеспечению стабильности данной процедуры позволят сделать ее применение более масштабным и эффективным.

Список литературы

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета. 25.12.1993. № 237.
2. О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва: Федеральный закон от 29.05.2019 № 103-ФЗ // Собрание законодательства. 03.06.2019. № 22. Ст. 2659.
3. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 23.05.2020 № 154-ФЗ // Собрание законодательства. 25.05.2020. № 21. Ст. 3233.
4. О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва: закон города Москвы. URL: www.mos.ru (дата обращения: 10.09.2022).
5. Алексеев Р. А. Блокчейн как избирательная технология нового поколения – перспективы применения на выборах в современной России // Вестник Московского государственного областного университета. 2018. С. 3–10.

6. Босова Е. Н., Реут Е. Н. Дистанционное электронное голосование: поиск законодательного оформления // Правоприменение. 2019. Т. 3, № 3. С. 53–62.

7. Федоров В. И., Ежов Д. А. Эволюция электронного голосования в России: проблемы классификации и периодизации // Вестник Московского государственного областного университета. 2021. № 21. С. 146–161.

8. URL: www.rcoit.ru (дата обращения: 10.09.2020).

А. А. Аракелян,

студент,

Институт государства и права,

Сургутский государственный университет

МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ: ВИКТИМОЛОГИЧЕСКАЯ ПРОФИЛАКТИКА

Аннотация. Мошенничество в сети Интернет на сегодняшний день является одним из самых распространенных видов хищения, с которыми сталкиваются пользователи социальных сетей. Во время пандемии люди стали больше времени проводить в интернет-пространстве, вследствие чего уровень мошенничества возрос. В ходе анализа статистики преступлений в данной сфере нами был выявлен ряд критериев, которые помогут удостовериться в добросовестности продавца, и составлен специальный алгоритм, который позволит минимизировать риски потери своего имущества.

Ключевые слова: мошенничество, социальные сети, интернет-пространство, хищение, пользователи сети Интернет, фальсифицированный аккаунт

FRAUD ON THE INTERNET: VICTIMOLOGICAL PREVENTION

Abstract. The article tells about Internet fraud. Nowadays, this type of crime is one of the most popular among users of the Internet space. During the pandemic, people began to spend more time on the Internet, as a result of which the level of fraud increased. In the article, after analyzing the statistics of crimes in this sphere, we identified a number of criteria that will help to verify the integrity of the seller, and compiled a special algorithm that will minimize the risks of losing people's property.

Keywords: Fraud, Social networks, Internet space, Theft, Internet users, Falsified account

Интенсивное и непрерывное развитие технологий порождает ряд негативных последствий для пользователей сети Интернет. В частности, мошенничества, совершенных с помощью глобальной сети Интернет.

Актуальность темы обуславливается тем, что мошенничество в сети Интернет на сегодняшний день является одним из распространенных видов хищения, с которыми сталкиваются пользователи. Во время пандемии люди стали больше

времени проводить в Интернет пространстве, вследствие чего уровень мошенничества возрос.

В большинстве случаев люди сами предоставляют мошенникам информацию, с помощью которой они незаконно переводят денежные средства на указанные им счета. Такое стало возможным в результате излишней доверчивости граждан к информации от незнакомых лиц, поспешности в принятии решений и личной безответственности.

Во избежание мошенничества в сети Интернет стоит несколько раз перепроверить аккаунт на наличие признаков фальсификации. В ходе анализа случаев мошенничества в социальной сети нами был выявлен ряд критериев, которые помогут удостовериться в добросовестности продавца, и создан алгоритм, который позволит минимизировать риски столкновения с мошенничеством в интернет-пространстве.

1. Необходимо изучить товар, который вы хотите купить на нескольких платформах, и выявить его среднюю стоимость. Если вы увидели, что стоимость товара не сильно отличается, то стоит проверить страницу по остальным критериям. Если стоимость товара значительно ниже, чем у других продавцов, то стоит насторожиться и уточнить причину такого ценообразования.

2. Обратите внимание на количество публикаций и постов, их давность. Если публикаций много и они систематически ведутся больше года, то вероятность мошенничества низкая, но все же не стоит торопиться. Если публикаций мало, либо их выставляли относительно недавно, то вероятность быть обманутым мошенником увеличивается.

3. Общие друзья или подписчики. Возможно, кто-то из ваших друзей уже осуществлял покупку в данном магазине. В таком случае, вы можете связаться с ним, убедиться в добросовестности продавца, и заказать нужный вам товар. Если общих знакомых нет, стоит обратить внимание на реальность количества подписчиков, также не стоит забывать о накрутке.

4. Проверьте отзывы других покупателей. Если на странице есть отзывы, их много и они положительные, то вы можете спокойно заказывать товар у данного продавца. Если отзывов нет, то лучше не подвергать свое имущество риску.

5. Оплата. Если оплату просят совершать предоплатой в 100 %-м размере, то стоит все же поискать более безопасный вариант. Если продавец просит внести предоплату в размере менее 50 %, или предлагает отправить товар наложенным платежом, то данный способ дает больше гарантий и позволит в определенной степени обезопасить себя от мошенников.

Таким образом, в социальных сетях злоумышленникам не составит труда выдать себя за другого человека или замаскироваться под известный бренд, чтобы завоевать ваше доверие, поэтому грамотное использование представленного алгоритма поможет вам избежать мошенничества в сети Интернет. Совершая покупки в социальных сетях, нужно быть внимательным и осмотрительным, проверять аккаунты продавцов на наличие признаков фальсификации, чтобы избежать хищения своего имущества.

Список литературы

1. Гридина Ю. А., Русскова А. А. Киберпреступность как новая криминальная угроза // Интеллектуальные ресурсы – региональному развитию. 2019. Т. 5, № 2. С. 299–304.
2. Гладкий А. Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников. Москва, 2018. С. 899–903.
3. Каткова М. Н. Профилактика виктимности в сети Интернет. Киров: Университет имени О. Е. Кутафина (МГЮА), 2018. С. 10–12.
4. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская академия МВД России, 2018. С. 5–8.
5. Романов С. А. Мошенничество в России. 1000 способов как уберечься от аферистов. Москва: Конец века, 2018. С. 320. URL: <https://www.litmir.me/br/?b=23505&p=1> (дата обращения: 15.09.2022).
6. Фатахова Д. Р. Мошенничество в сети Интернет // Молодой ученый. 2020. № 49 (339). С. 341–344.
7. Шейнов В. П. Как защититься от обмана и мошенничества: монография. Москва: Харвест, 2019. С. 464–466.

А. А. Арланова,
старший преподаватель,
кафедра цифровой экономики,
Туркменский государственный институт экономики и управления

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ СИСТЕМЫ ТУРКМЕНИСТАНА

Аннотация. В данной работе рассматривается вопрос развития приоритетных направлений в финансово-экономической системе Туркменистана, основные направления роста и этапы внедрения технологий в экономику страны. Проведен системный анализ развития цифровых технологий и их влияния на развитие финансово-экономических систем. Даны рекомендации по внедрению технологий в финансовое регулирование страны и процесса бюджетирования.

Ключевые слова: цифровая экономика, финансы, технологии

PRIORITY AREAS OF DIGITAL TRANSFORMATION OF THE FINANCIAL AND ECONOMIC SYSTEM OF TURKMENISTAN

Abstract. In this paper, the issue of the development of priority areas in the financial and economic system of Turkmenistan, the main directions of growth and the stages of introducing technologies into the economy of Turkmenistan were considered. A systematic and analytical analysis of the development of digital technologies and their impact on the development of financial and economic systems was carried out. Recommendations are given on the introduction of technologies in the financial regulation of the country and the budgeting process.

Keywords: Digital economy, Finance, Technology

В период Возрождения новой эпохи могущественного государства в Туркменистане [8] проводятся огромные работы по поэтапному развитию цифровой экономики, обеспечению высокой инвестиционной активности, укреплению экспортного потенциала страны, увеличению производства импортозамещающей продукции, повышению эффективности социальных систем, укреплению сотрудничества государства и частного сектора. В развитии цифровой экономики первое место отведено финансово-экономическому и банковскому секторам, государственному управлению, которые стремительно адаптируются к цифровым трансформациям и сегодня дают четкие результаты [1. С. 59].

Правительство и общество, предприятия и бизнес-среда, потребители ожидают огромных результатов от цифровизации экономики. Результатом здесь является предоставление доступа к цифровым продуктам и цифровым сервисам, порталам и платформам, программам и приложениям, внедрение интеллектуальных технологий и инновационных бизнес-моделей. Безусловно, с переходом к цифровой экономике появилось несколько направлений, некоторые из которых получили развитие, такие как: онлайн-сервисы, онлайн-покупки, электронные платежи, интернет-реклама или цифровая реклама, электронный документооборот, онлайн-мониторинг, краудфандинг и др. [2. С. 62]

Цифровизация всех отраслей Туркменистана, в первую очередь финансово-экономических систем, является основным вектором развития страны за последние несколько лет. Сохранится тенденция и в будущем. На сегодняшний день финансово-экономическая система является одним из самых динамично развивающихся направлений Туркменистана.

В качестве основных целей использования цифровых технологий в экономике можно отметить: анализ текущих макро- и микроэкономических показателей в результате создания экосистем, связанных с финансово-экономическими институтами за счет использования интеллектуальных технологий, а также создание возможности принимать эффективные решения и точно прогнозировать ожидаемые результаты будущей деятельности, формирование цифровой инвестиционной среды для компаний, разрабатывающих новые технологии и продукты и т. д. [3. С. 80].

Велико значение цифровых технологий и в финансовой сфере. В настоящее время в отечественной и международной практике разрабатываются и внедряются технологии, направленные на предоставление финансовых услуг с использованием ряда интеллектуальных и инновационных технологий, таких как большие данные, искусственный интеллект, машинное обучение, робототехника, блокчейн и облачные вычисления, биометрия. Такие технологии в мировой практике называются FinTech (Financial Technology – «финансовые технологии»). Финтех относится к инновациям и разработкам в сфере финансовых услуг, которые повышают доступность финансовых и банковских услуг для широкой общественности и бизнес-среды. Основными целями развития финансовых технологий являются:

- обеспечение доступности финансовых услуг, увеличение их видов и повышение качества;
- снижение рисков и издержек в финансовой системе;
- повышение конкурентоспособности финансовых технологий;

- обеспечение безопасности и стабильности при использовании финансовых технологий, обеспечение кибербезопасности (биометрическая система распознавания личности позволяет защитить данные, сеть и приложения финансовых учреждений);
- создание финансовой экосистемы (онлайн-сервисы, интегрирующие информацию о товарах, сервисах, клиентах, рекламе и доходах компании) [4. С. 52].

Особенности приоритетных интеллектуальных технологий в финансово-экономической сфере:

- Алгоритмы искусственного интеллекта используются для прогнозирования состояния фондового рынка и анализа экономических условий. Искусственный интеллект также является услугой, доступной финансовым учреждениям для сбора данных о наиболее частых действиях своих клиентов и более глубокого их изучения.

- Большие данные используются для прогнозирования инвестиций клиентов и изменений рынка, создания новых стратегий и портфелей. Большие данные также используются для предотвращения мошенничества, оптимизации маркетинговых стратегий банков и компаний.

- Блокчейн – интеллектуальная технология, используемая для обеспечения надежности и безопасности регистрации и хранения информации о транзакциях, осуществляемых в финансовых и банковских системах, позволяющая управлять рисками и заключать договоры [5. С. 91].

Основываясь на отечественный и мировой опыт, можно отметить основные направления использования цифровых финансовых технологий (FinTech) в финансово-банковской системе и их совершенствования:

- Очень быстрые кредитные операции (оперативное кредитование). Например, «кредиты до зарплаты», которые не используются банками. На сегодняшний день населению предлагается одна из финансовых новинок, внедряемых кредитными организациями Туркменистана, – услуга овердрафтного кредита.

Электронные платежные системы. На сегодняшний день, ориентируясь на международный опыт, наряду с национальными платежными системами, кредитными организациями Туркменистана внедрены и совершенствуются различные виды цифровых платежных услуг.

Цифровые банковские технологии для предоставления финансовых услуг с использованием мобильных и онлайн-платформ. Эта технология экономит затраты и время, повышает безопасность персональных данных, качество и скорость обслуживания, а также предоставляет все банковские услуги в онлайн-режиме через онлайн-порталы и банковские приложения.

Цифровые решения для финансовых услуг. В связи с этим в мировом опыте существует множество технологий, например, дебетовая карта с дактилоскопическим датчиком (сканером отпечатков пальцев) для повышения удобства оплаты (Норвегия); технология идентификации клиентов банка с помощью голосовой биометрии в режиме реального времени (онлайн) во время телефонного разговора с оператором контакт-центра (Израиль); цифровые помощники на сайте банка (консультации, обучение клиентов, поиск более успешных кандидатов), т. е. чат-боты (Россия).

Интегрированная сервисная платформа с использованием Big Data для анализа бизнес-конъюнктуры малых и средних предприятий (онлайн-сервис США SizeUP).

Эта платформа учитывает различные факторы: сравнивает доходы компании, анализирует ее общее развитие и предоставляет услугу по оптимизации рекламы.

Создание цифрового профиля. Цифровые профили используются кредитными, страховыми, микрофинансовыми организациями и торговыми площадками.

Разработка «Открытого API» – универсального интерфейса, обеспечивающего доступ к данным для организации платежных услуг финансовых учреждений и различных компаний.

Создание небанков. Необанк – финансовое учреждение, работающее только в Интернете; финансовые учреждения, предоставляющие банковские услуги дистанционно только в цифровом формате (мобильное приложение и сайт). Небанки особенно заинтересованы в современных цифровых технологиях, позволяющих обрабатывать большие объемы данных и предоставлять услуги населению.

Разработка механизма удаленной идентификации клиентов с использованием единой унифицированной биометрической системы [6. С. 15].

Уместно отметить, что на III этапе (в 2024–2025 гг.) Концепции развития цифровой экономики в Туркменистане на 2019–2025 гг. определено продолжить совершенствование и внедрение цифровых интеллектуальных технологий и методов в различные отрасли экономики страны. Также, как сказано в части ожидаемых результатов от реализации Концепции, они обеспечат дополнительное развитие системы ИКТ в ВВП страны, будут развиваться новые виды бизнеса, включающиеся в международный производственный цикл, будут формироваться новые виды привлечения инвестиций в цифровую экономику; с широким внедрением цифровых технологий повысится качество банковских услуг, будут созданы новые современные виды услуг, основанные на экономии затрат и времени; более широкое распространение получат безналичные расчеты, основанные на международном опыте и передовых технологиях.

В условиях цифровой экономики банки Туркменистана стремительно совершенствуют услуги интернет-банкинга и мобильного банкинга, а также увеличивают спектр и виды цифровых услуг. В настоящее время с развитием электронного бизнеса и электронной коммерции в стране возрастает значение электронных платежных систем, в связи с этим внедряются соответствующие технологии, обеспечивающие качество и оперативность дистанционных цифровых банковских услуг, в том числе технологии удаленной идентификации, создание цифрового профиля и регистрация финансовых транзакций на основе искусственного интеллекта. Эти технологии были разработаны и подготовлены с учетом технологических, маркетинговых и экономико-организационных аспектов.

Помимо этих возможностей, перед нами стоят очень важные задачи, наряду с мероприятиями, реализуемыми в экономике, финансовой и банковской системах страны. Важны разработка и тестирование цифровых сервисных платформ и цифровых решений на основе углубленного изучения ведущих методик мирового опыта и отечественных подходов; продолжение внедрения и постоянного улучшения интеллектуальных технологий, таких как искусственный интеллект, большие данные, блокчейн и облачные технологии. Например, в мировой практике функционирует единая цифровая система налоговой информации. Данная система активизирует

взаимодействие и обмен информацией между налоговым органом и предпринимателями, банковской системой в целом, налогоплательщиками, в том числе обеспечивает мониторинг платежных документов, оперативный и онлайн-анализ продаж, маркировку товаров и работу с маркированными товарами, облегчает и уточняет их контроль, обеспечивает конфиденциальность и защиту данных [7. С. 197].

Список литературы

1. Аброскин А. С. Международный опыт измерений цифровой экономики // Вестник университета. 2018. № 12. С. 59–60. URL: <https://elibrary.ru/item.asp?id=36963747>
2. Ахметова С. Г., Невская Л. В. Опыт внедрения новых технологий в высшем профессиональном образовании // Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. 2018. № 2. С. 62–69. URL: <https://elibrary.ru/item.asp?id=35193981>
3. Багаутдинова Н. Г., Никулин Р. А. Новые конкурентные преимущества в условиях цифровизации // Инновации. 2018. № 8. С. 80–83.
4. Барабаш К. С. Влияние цифровой экономики на изменение рынка труда // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2018. № 6 (97). С. 52–54.
5. Баранов Д. Н. Социально-экономические последствия распространения цифровых технологий на рынке труда // Вестник Московского университета им. С. Ю. Витте. Серия 1: Экономика и управление. 2018. № 3 (26). С. 91–97.
6. Баранов Д. Н. Сущность и содержание категории «цифровая экономика» // Вестник Московского университета им. С. Ю. Витте. Серия 1: Экономика и управление. 2018. № 2 (25). С. 15–23.
7. Большаков С. В. Актуальные проблемы корпоративных финансов в цифровой экономике // РИСК: Ресурсы. Информация. Снабжение. Конкуренция. 2018. № 4. С. 197–203.
8. Программа Возрождение новой эпохи могущественного государства: Национальная программа социально-экономического развития Туркменистана в 2022 – 2052 гг. Утв. Президентом Туркменистана. URL: <https://turkmenistan.gov.tm/index.php/ru/post/60781/utverzhdena-programma-vozhrozhdenie-novoj-epohi-mogushchestvennogo-gosudarstva-nacionalnaya-programma-socialno-ekonomicheskogo-razvitiya-turkmenistana-v-2022-2052-godah>

А. А. Арланова,
старший преподаватель, кафедра цифровой экономики,
Туркменский государственный институт экономики и управления
М. Чарыев,
студент,
Туркменский государственный институт экономики и управления
О. Дурдыев,
студент,
Туркменский государственный институт экономики и управления

ИННОВАЦИОННЫЕ РЕФОРМЫ ЦИФРОВИЗАЦИИ ЭНЕРГЕТИЧЕСКОГО СЕКТОРА ТУРКМЕНИСТАНА

Аннотация. Рассмотрен вопрос развития приоритетных направлений в энергетическом секторе Туркменистана, а также роль технологий в развитии энергетического сектора и будущее планирование развития технологий. Проведен системный и аналитический анализ развития цифровых технологий в энергетическом секторе Туркменистана. Даны рекомендации по внедрению технологий в отрасль, их особенности и проблемы развития.

Ключевые слова: цифровая экономика, энергетика, технологии

INNOVATIVE REFORMS OF DIGITALIZATION OF THE ENERGY SECTOR OF TURKMENISTAN

Abstract. In this paper, the issue of developing priority areas in the energy sector of Turkmenistan, as well as the role of technology in the development of the energy sector and future planning for the development of technologies, was considered. A systematic and analytical analysis of the development of digital technologies in the energy sector of Turkmenistan was carried out. Recommendations are given on the introduction of technologies into the industry, their features and problems of development.

Keywords: Digital economy, Energy, Technology

В настоящее время страны мира уделяют большое внимание цифровизации, считая, что от использования цифровых технологий зависит будущий уровень экономического развития. С этой точки зрения, в рамках реализации «Концепции развития цифровой экономики в Туркменистане на 2019–2025 годы» проводится масштабная работа по внедрению цифровых, высокотехнологичных и информационных технологий во все отрасли экономики страны. Принятие Концепции дало мощный толчок инновационному развитию экономики страны. Она направлена на повышение эффективности всех отраслей экономики за счет использования инновационных технологий, ускорение процесса перехода национальной экономики на путь инновационного развития, а также внедрение в производство передовых технологий [1. С. 59].

Государственная политика направлена на развитие экономики путем диверсификации за счет комплексных реформ и внедрения цифровой системы в отрасли народного хозяйства, широкое внедрение принципов рыночных отношений, вхож-

дение нашей страны в число промышленно развитых стран. Внедрение цифровой экономики будет способствовать внедрению цифровых технологий, способствующих долгосрочному развитию экономики и высокой производительности труда в стране, повышению качества государственных услуг и установлению усовершенствованных форм, обеспечению сокращения рисков, связанных с технологиями реформирования условий жизни народа [2. С. 62].

В этом контексте успешно проводится работа по внедрению цифровой экономики во все отрасли нашего региона, которые развиваются на основе инновационных технологий. Электроэнергетика также играет важную роль в реализации запланированных программных работ по цифровизации промышленности нашей страны. Цифровая энергетика, являясь составной частью цифровой экономики, включает в себя оснащение всех отраслей топливно-энергетической системы современными цифровыми технологиями и технологическим оборудованием, т. е. определяется как новый тип управления функционированием системы [3. С. 80].

Умные энергосистемы (smart grid) – это модернизированная электросеть, которая использует информационные и коммуникационные сети и технологии для сбора данных о производстве и потреблении энергии для автоматического повышения экономических выгод, эффективности, надежности и устойчивого производства и распределения электроэнергии.

Умные энергосистемы – это электрическая сеть, которая включает в себя множество практических и энергетических потенциалов, таких как умные счетчики, умные переключатели, интеллектуальные устройства и приложения, возобновляемые источники энергии и энергоэффективность [4. С. 52].

Этот термин в 2003 г. впервые был упомянут в научной статье Майкла Т. Берра. Сегодня электроэнергетика трансформируется по трем направлениям:

- улучшение инфраструктуры;
- добавление цифрового слоя, формирующего ядро «умной сети»;
- трансформация бизнес-процессов, делающая интеллектуальную сеть рентабельной [5. С. 91].

Хотелось бы отметить, что Туркменистан является одной из самых богатых стран мира по запасам энергоресурсов, а производство электроэнергии считается одной из самых востребованных отраслей в мире. Государственная политика в сфере энергетики состоит в обеспечении энергетической независимости и безопасности, повышении эффективности потребления электроэнергии, внедрении в производство новых цифровых технологий на основе снижения его негативного воздействия на окружающую среду [6. С. 15].

Основными задачами цифровизации электроэнергетики, т. е. внедрения цифровых технологий, являются:

- анализ потерь и других затрат в электроэнергетике;
- улучшение возможностей электронного сбора, агрегирования и обмена данными об использовании энергии с удаленных устройств;
- создание условий для использования учреждениями, предприятиями и организациями, а также гражданами альтернативных источников энергии;

- создание условий для привлечения компаний, специализирующихся на производстве энергии с использованием цифровых систем из возобновляемых и неисчерпаемых ресурсов;
- создание условий для увеличения объемов внедрения приборов измерения электроэнергии;
- развитие точек сети общественного пользования, предназначенных для питания устройств мобильной связи (в том числе на основе солнечной энергии);
- расширение внедрения энергосберегающих и дистанционно управляемых столбов освещения на улицах;
- привлечение частных инвестиционных средств для внедрения цифровых технологий в электроэнергетике;
- экономия времени на подключение к системам энергоснабжения за счет развития электронного документооборота.

Реализуя крупномасштабные проекты регионального и международного значения в сфере энергетики, Туркменистан показывает, что к вопросам охраны окружающей среды нужно подходить на очень высоком уровне. В этом контексте в нашей стране также очень ответственно подходят к вопросам охраны окружающей среды. Одной из основных задач «Концепции развития цифровой экономики в Туркменистане на 2019–2025 годы» является внедрение энергосберегающих и экологически безопасных цифровых технологий. В связи с этим особое внимание уделяется разработке инновационных, экологически чистых, энергосберегающих технологий, направленных на использование энергии природных ресурсов (солнца, ветра, водного и гидротермального тепла, биогаза). Активное внедрение в промышленность энергосберегающих, экологически чистых технологий является основным направлением социально-экономических программ, непрерывно реализуемых под руководством уважаемого Президента.

В целях внедрения в энергетику нашей страны новейших достижений науки и мировой практики проводятся соответствующие мероприятия. То есть сегодня в стране успешно реализуются масштабные проекты в области энергетики, непрерывно устанавливаются системы электропередачи, строятся распределительные станции, все уголки страны эффективно снабжаются электроэнергией. В результате туркменская энергетика стремительно развивается и способна увеличивать экспорт электроэнергии, востребованной на мировом рынке [7. С. 197].

В целях обеспечения бесперебойного снабжения электроэнергией новых промышленных и социальных объектов в стране принимаются соответствующие меры. Это отражено в Концепции «Умного города», реализуемой в настоящее время под руководством Президента. Задачи «Умного города» направлены на обеспечение всех жилых комплексов и зданий сенсорными системами с целью снижения энергопотребления, а также их безопасности и автономности. То есть будут контролироваться «умные» системы, установленные в домах, отопление и освещение помещений, примерное количество энергии, потребляемой используемыми в быту приборами, недопущение чрезмерного энергопотребления. А в производстве рассматривается использование экологически чистых источников энергии, таких как солнце, вода и ветер.

Собственно говоря, у мегапроекта «Ашхабад-Сити» есть официальный сайт в сети Интернет: <https://ashgabatcity.gov.tm/>. На сайте размещены краткое описа-

ние «города в городе», позволяющее ознакомиться с проектами будущих жилых комплексов, интерактивная онлайн-карта «Ашхабад-сити» 3D с возможностью виртуального тура по карте.

Таким образом, внедрение цифровых технологий в энергосистему страны в дальнейшем послужит прочной основой для глубокой модернизации отрасли и современного развития систем производства и жизнедеятельности. Это также приведет к повышению производительности труда, снижению себестоимости продукции, повышению эффективности и конкурентоспособности отрасли, росту кооперации, высоким результатам экономического развития, укреплению энергетического потенциала нашей страны.

Список литературы

1. Аброскин А. С. Международный опыт измерений цифровой экономики // Вестник университета. 2018. № 12. С. 59–63. <https://elibrary.ru/item.asp?id=36963747>
2. Ахметова С. Г., Невская Л. В. Опыт внедрения новых технологий в высшем профессиональном образовании // Вестник Пермского национального исследовательского политехнического университета. Социально экономические науки. 2018. № 2 . С. 62–69. URL: <https://elibrary.ru/item.asp?id=35193981>
3. Багаутдинова Н. Г., Никулин Р. А. Новые конкурентные преимущества в условиях цифровизации // Инновации. 2018. № 8. С. 80–83.
4. Барабаш К. С. Влияние цифровой экономики на изменение рынка труда // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2018. № 6 (97). С. 52–54.
5. Баранов Д. Н. Социально-экономические последствия распространения цифровых технологий на рынке труда // Вестник Московского университета им. С. Ю. Витте. Серия 1: Экономика и управление. 2018. № 3 (26). С. 91–97.
6. Баранов Д. Н. Сущность и содержание категории «цифровая экономика» // Вестник Московского университета им. С. Ю. Витте. Сер. 1, Экономика и управление. 2018. № 2 (25). С. 15–23.
7. Большаков С. В. Актуальные проблемы корпоративных финансов в цифровой экономике // РИСК: Ресурсы. Информация. Снабжение. Конкуренция. 2018. № 4. С. 197–203.

А. Н. Артамонов,

кандидат юридических наук,

Главное управление Минюста России по Ростовской области

ИЗМЕНЕНИЕ ТРАДИЦИОННЫХ СПОСОБОВ КОММУНИКАЦИИ КАК БЛАГО И ТРАДИЦИОННЫХ ЦЕННОСТЕЙ КАК ПУТЬ В БЕЗДНУ

Аннотация. В статье на основе анализа практики оказания международной правовой помощи, мониторинга тенденций и характера особых видов записей актов гражданского состояния обозначаются проблемы действующего российского законодательства и обосновывается необходимость обсуждения и выработки путей решения спорных правовых и морально-этических вопросов.

Предлагается отменить нормативные правовые акты, способствующие упрощенной процедуре регистрации однополых браков, высказывается необходимость широкого обсуждения возникающих проблем.

Ключевые слова: международное сотрудничество, цифровизация, новые технологии, запись акта гражданского состояния, заключение о перемене пола, Минюст России, юридически значимый факт

CHANGING TRADITIONAL WAYS OF COMMUNICATION AS A BLESSING AND TRADITIONAL VALUES AS A PATH TO THE ABYSS

Abstract. Based on an analysis of the practice of providing international legal assistance, some elements of digitalization and problems associated with its absence, monitoring trends and the nature of certain types of civil status records, the article identifies the problems of the current Russian legislation and suggests the need to discuss and develop ways to resolve ambiguous legal and moral-ethical issues. It is proposed to abolish the normative legal act that contributes to the simplified procedure for registering same-sex marriages, the need is expressed for the discussion of the problem to involve specialists not only from the legal community, but also from all caring citizens.

Keywords: International cooperation, Digitalization, New technologies, Registration of a civil status act, Conclusion on gender reassignment, Ministry of Justice of Russia, Legally significant fact

Введение. Современное право остается пока в традиционном его понимании, способах создания и применения, притом что подвержены активному изменению методы передачи, хранения, возможности использования информации, имеющей правовые последствия. Это порождает опасения об искажении, фальсификации, формах воздействия на принимаемые человеком решения с использованием новых технологий.

Наряду с увлечением разработкой и внедрением новых технологий, мы порой уделяем недостаточно внимания сохранению традиционных ценностей, не предпринимаем должных усилий по их защите, не просчитываем перспективы их изменения или замены новыми, «модными», позволяем себе заигрывать с их сторонниками.

Все это, безусловно, подчеркивает актуальность осмысления перспектив цифровизации, искусственного интеллекта, их безопасности для человека и возможностей контроля с его стороны, параллельно обсуждая преимущества, предоставляемые данными новшествами, наряду с повышением необходимости сохранения лучших традиций, выработанных человечеством.

Основная часть. Для описания современной практики и нормативной базы, в том числе международных соглашений об истребовании личных документов, подтверждающих юридически значимые факты и имеющих значение для обретения соответствующих статусов человека: гражданства, получения пенсии, вступления в наследство и т. д., – приведем некоторые ответы, данные гражданам на запросы по вопросам международного сотрудничества.

Так, на запрос гражданина Украины, проживающего на территории Российской Федерации и запросившего документы с территории Украины для решения вопроса получения российского гражданства (вопрос сейчас актуальный, не носящий единичный или редкий характер и имеющий отдаленные, в том числе политические, последствия), Главным управлением Минюста России по Ростовской области был дан ответ о невозможности осуществления такого запроса документов в соответствии с тем, что, согласно письму филиала АО «Почта России» по Ростовской области, «Почта России» временно прекратила прием отправок на Украину в связи с остановкой работы «Укрпошты» и закрытием прямого почтового обмена между странами. Актуальную информацию об ограничениях почтового обмена с другими странами мира можно узнать на сайте «Почты России», при этом Главное управление Минюста готово оказать содействие в препровождении материалов украинской стороне в случае возобновления «Почтой России» приема отправок на территорию Украины.

И второй ответ, точнее, также отказ в истребовании документов – справки о наличии (отсутствии) гражданства Республики Казахстан. Заявителю было разъяснено, что порядок истребования личных документов на территории Российской Федерации предусмотрен Административным регламентом Министерства иностранных дел Российской Федерации и Министерством юстиции Российской Федерации, утвержденным совместным приказом от 29.06.2012 № 10489/124. Данным регламентом предусмотрено, что для истребования документов о стаже работы заявитель представляет в компетентный орган (Главное управление Минюста России по соответствующему субъекту Российской Федерации) заявление об истребовании документа, копию паспорта или иного документа, удостоверяющего личность заявителя в соответствии с законодательством Российской Федерации. Заявление заполняется с применением компьютерной, машинописной техники либо разборчивым почерком (не допускается исправление ошибок путем зачеркивания и с помощью корректирующих средств). Заявление должно быть подписано заявителем (доверенным лицом), в последнем случае в пакете документов должна быть доверенность, удостоверенная в установленном порядке.

Такое подробное изложение характера ответов заявителям на запросы по оказанию международной правовой помощи позволяет передать суть проводимой работы и проблем или препятствий, которые стоят на пути подтверждения тех или иных юридически значимых фактов. Они заключаются в способах коммуникации, допускаемых при оказании такого вида государственных услуг (только почтовое сообщение), и в отсутствие каких-либо интегрированных баз – все должно быть подтверждено бумажным документом, в случае необходимости еще и заверенного соответствующим образом.

Наверное, не совсем своевременно сейчас, на фоне все более рассыпающихся различных межгосударственных взаимоотношений, обсуждать подобные проблемные вопросы – стоит радоваться, что какие-то способы коммуникаций остаются, что позволяет обеспечивать часть гражданских прав и законных интересов. Однако, с другой стороны, возможно, нынешняя общественно-политическая,

международно-правовая обстановка и позволит нам отказаться от традиционной инертности в изменении каких-то сложившихся, устоявшихся положений и одновременно показать пример новых возможностей с теми субъектами международного права, с которыми развитие отношений набирает положительный оборот и обретает новые активные формы.

Мы уже не первый год переходим на иные формы коммуникации, когда материальная доставка послания, информации путем физической передачи из рук в руки заменяется электронными средствами, что широко распространяется на различные вопросы и сферы общественных отношений внутри нашей страны, но трудно выходит за ее пределы (во всяком случае официальный документооборот). Однако есть и такие примеры, когда, пока отдельные государства пробуют внедрять новые возможности, в том числе в международно-правовую сферу, примером чему может служить недавняя Нота Посольства Республики Чили в РФ относительно использования Республикой Чили системы электронного апостиля (легализации документов, представляемых на территории иностранного государства).

Вопросам цифровизации, внедрению новых технологий, а как следствие, новых возможностей для человека в последние годы уделялось много внимания, подавляющее большинство описаний таких перспектив или уже реальности преподносилось как однозначное благо, обеспечивающее только дополнительные возможности реализации прав граждан и их законных интересов.

Нынешняя же реальность показывает, что и государственный суверенитет, и личная информационная, а значит, и всякая иная безопасность человека от цифровизации и внедрения подобных технологий далеко не всегда выигрывает.

Под руководством Минюста России отечественными загсами в 2020 г. была проведена огромная по объему работа по оцифровке записей актов гражданского состояния: рождений, смертей, регистраций браков и разводов, перемены имени и т. д., что, безусловно, облегчило участь многих из нас в различных сферах жизнедеятельности (подтверждение юридически значимых фактов) – многие решения теперь могут приходиться к нам автоматически, что нами (всеми, кто не слишком интересуется вопросами конспирологии или утраты духовности через применение новых технологий) воспринято как абсолютное добро или благо.

При этом результаты проведенного Главным управлением Минюста России по Ростовской области совместно с Управлением ЗАГС Ростовской области заставляют задуматься и даже засомневаться в каких-то вещах, которые раньше считались однозначными. Что-то же влияет на наши взгляды, действия, принимаемые решения – и это не только несовершенство законодательства, различные его лазейки, отсутствие суровости наказания и прочие наши традиционные предложения по изменению (улучшению) общественных отношений.

Например, по информации Управления ЗАГС Ростовской области, на территории Ростовской области за последние 25 лет было составлено 57 заключений о внесении изменений в запись акта гражданского состояния в соответствии со ст. 70 Федерального закона от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния». Согласно указанной статье (в редакции Федерального закона 2013 г.),

заклучение о внесении исправлений или изменений в запись акта гражданского состояния составляется органом записи актов гражданского состояния в случае, если представлен документ об изменении пола, выданный медицинской организацией по установленной форме и в соответствующем порядке.

Интересна тенденция составления таких заключений: так, за 20 лет, с 1997 по 2017 г. их было оформлено 12 (восемь граждан изменили пол с женского на мужской, их возраст – от 23 до 43 лет). За неполных четыре года, с 2018 г. по настоящее время (вторая половина 2022 г.), таких записей составлено уже 45 (26 человек изменили пол с женского на мужской, 19 – с мужского на женский, возраст составил от 18 до 51 года).

2018 г. породил такой всплеск заключений о перемене пола в связи с вступлением в силу положений приказа Минздрава России № 850н, утвердивших форму и порядок выдачи медицинской организацией документа об изменении пола.

Аналогичная статистика и с переменной имени по заявлению лиц, изменивших пол: за 20 лет, с 1997 по 2018 г., – восемь записей актов, за неполных четыре года, с 2018 по середину 2022 г., – 32.

Дальше статистика предоставляет еще больше поводов удивиться, изумиться или проявить другую эмоцию (надеемся, однозначно негативную): после изменения пола и перемены имени 11 граждан зарегистрировали заключение брака (по одному в 1997, 2005, 2020, два – в 2019 и уже шесть – в 2022 г.). Фактически речь идет о заключении однополых браков, юридическим основанием которых является лишь измененная запись в акте гражданского состояния, а субъект этих правоотношений каким был при рождении, таким и остался.

Интерес вызывает также статистика обращений граждан в органы ЗАГС Ростовской области по вопросам разъяснения положений российского законодательства, регулирующего оформление документов в связи с изменением пола, трансгендерных переходов: 31 обращение (с 1997 по 2017 г. – 6 обращений, с 2018 г. по настоящее время – 25).

Может ли и должна ли вызывать беспокойность приведенная статистика? На наш взгляд, безусловно. Во-первых, это цифры только одного субъекта Российской Федерации, а их, напомним, по нашей Конституции 85 (и, надеемся, в ближайшем будущем будет еще больше), во-вторых, пугает взрывной рост статистических показателей за последние неполных четыре года. Объясняется последнее очень просто: с 2018 г. (вступление в силу положений указанного выше приказа Минздрава России) справка об изменении пола выдается гражданам врачебной комиссией медицинской или иной организации, осуществляющей медицинскую деятельность на основании лицензии, предусматривающей выполнение работ (услуг) по психиатрии.

В состав такой комиссии (по установлению половой переориентации) должен входить врач-психиатр, врач-сексолог и медицинский психолог, а направление на нее выдается врачом-психиатром по результатам медицинского наблюдения гражданина в случае установления ему диагноза «транссексуализм». Таким образом, справку могут получить граждане, не прошедшие гормональную терапию и хирургическую коррекцию пола (т. е. «каким ты был, таким ты и остался»), и никаких сложностей ее получение на практике не вызывает. Данная справка является

основанием для внесения сведений о половой принадлежности в записи акта о рождении гражданина, последующей перемене имени в органе ЗАГС и замене документа, удостоверяющего личность (паспорта), в органах МВД.

В результате таких преобразований на бумаге или в цифровом формате гражданин имеет право заключать брак, что является прямым нарушением положений Конституции Российской Федерации: основные права и свободы человека неотчуждаемы и принадлежат каждому от рождения (ст. 17), при этом в соответствии с российским законодательством семейные отношения осуществляются в брачном союзе мужчины и женщины, что относится к его основным началам (ст. 1 Семейного кодекса Российской Федерации).

Заключение. По результатам проведенного анализа практики регистрации изменения пола и связанных с ним других регистрационных действий на территории Ростовской области были сформулированы предложения об отмене приказа Минздрава РФ «Об утверждении формы и порядка выдачи медицинской организацией документа об изменении пола», а также о внесении изменения в ст. 70 Федерального закона «Об актах гражданского состояния», изложив абзац четвертый в следующей редакции» «представлен документ об изменении пола на основании хирургической коррекции и гормональной терапии, выданный медицинской организацией, осуществляющей медицинскую деятельность на основании лицензии, предусматривающей выполнение указанных услуг».

Данные предложения и возможная их реализация по корректировке действующего российского законодательства способна лишь немного затруднить процедуру изменения пола и ту ее легкость, что может провоцировать (с целью, например, поиграть в такие вещи или решить какие-то другие задачи, которые может обеспечить принадлежность к противоположному полу) соответствующие действия со стороны в первую очередь неокрепших умов.

Однако это не уберет саму проблему, которая отражается в статистике, приведенной нами выше, и в которой мы видим опасность для морали, нравственности и самой природы человеческой, глубину которой, возможно, мы сегодня не осознаем в полной мере. Нашей целью является обратить внимание на различные стороны нашей общественной жизни, на то, как юридическими методами, статистическими показателями возможно выявлять проблемные вопросы и тенденции их развития, а также привлечь к обсуждению, осмыслению причин и последствий специалистов иных отраслей знаний, чтобы не пропустить возможности повлиять на них и не допустить их необратимости и катастрофичности.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. 25.12.1993. № 237 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_196819/ (дата обращения: 05.09.2022).
2. Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ // Собрание законодательства Российской Федерации. 01.01.1996. № 1 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_18823/ (дата обращения: 07.09.2022).

3. Федеральный закон от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния» // «Российская газета». 20.11.1997 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_1778/ (дата обращения: 06.09.2022).

4. Приказ МИД России и Минюста РФ от 29.06.2012 № 10489/124 «Об утверждении Административного регламента Министерства иностранных дел Российской Федерации и Министерства юстиции Российской Федерации по предоставлению государственной услуги по истребованию личных документов» / Зарегистрирован в Минюсте РФ 25.07.2012, рег. № 25033 // «Российская газета». 24.08.2012. № 194 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_36787/ (дата обращения: 06.09.2022).

5. Приказ Министерства здравоохранения РФ от 23.10.2017 № 850н «Об утверждении формы и порядка выдачи медицинской организацией документа об изменении пола» / Зарегистрирован в Минюсте РФ 19.01.2018, рег. № 49695 // Официальный интернет-портал правовой информации (www.pravo.gov.ru). 22.01.2018. СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_45577/ (дата обращения: 05.09.2022).

М. А. Архангельская,
студент,

Казанский инновационный университет имени В. Г. Тимирязова

ИСПОЛЬЗОВАНИЕ 3D-ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ СУДЕБНО-МЕДИЦИНСКОГО ЭКСПЕРТА

Аннотация. В настоящее время существует множество видов 3D-технологий, имеющих серьезное значение для судебно-медицинской экспертизы. Некоторые системы 3D-сканирования уже активно используются в отделениях бюро судебно-медицинской экспертизы (СМЭ) России. Актуальность данной темы исследования обусловлена в первую очередь повышенным функционалом новых технологий, что существенно помогает судебно-медицинскому работнику в его деятельности. Также стоит отметить разнообразие технологических улучшений, которые с каждым годом требуют адаптации и интеграции их в рабочий процесс.

Ключевые слова: 3D-технологии, судебно-медицинский эксперт, виртопсия, стереолитография, судебно-медицинское исследование трупа, цифровизация, технологический прогресс

THE USE OF 3D TECHNOLOGIES IN THE ACTIVITIES OF A FORENSIC MEDICAL EXPERT

Abstract. Currently, there are many types of 3D technologies that are of serious importance for forensic medical examination. Some 3D scanning systems are already actively used in the offices of the Russian Bureau of the Ministry of Internal Affairs. The relevance of this research topic is primarily due to the increased functionality of new technologies, which significantly helps the forensic medical worker in his activities.

It is also worth noting the variety of technological improvements, which every year requires adaptation and integration into the workflow.

Keywords: 3D technologies, Forensic medical expert, Virtopsy, Stereolithography, Forensic medical examination of a corpse, Digitalization, Technological progress

Введение. Традиционно судебно-медицинские эксперты в проведении измерений полагаются на обычные аналоговые инструменты. Однако в практической деятельности телесные повреждения при применении таких предметов исследуется неточно, т. е. идет накапливание значительных производственных ошибок, что может привести к вынесению ложного заключения.

В ходе проведения судебно-медицинского исследования трупа эксперту существенную сложность представляет установление прижизненности и (или) давности причинения обнаруженных повреждений. Зачастую работник СМЭ оценивает давность повреждения мягких тканей преимущественно на основании морфологических изменений, выявленных визуально на макро-микроуровнях. Однако определить давность повреждений мягких тканей на основе одних только внешних признаков воспалительных реакций, например, отека, повышения температуры, весьма затруднительно, что связано с действием внешних и внутренних факторов. Так, на интенсивность процессов, протекающих в органах и тканях, существенную роль оказывают как экзогенные (температура окружающей среды, наличие и количество одежды и т. д.), так и эндогенные (степень и локализация повреждения, особенность кровообращения) проявления. Заметим, что ошибки в проведении судебно-медицинской экспертизы [4. С. 165] могут повлечь потерю или утрату важнейшей для дальнейшего расследования информации.

Основная часть. 3D-сканирование как технология, способствующая улучшению качества работы судебно-медицинского эксперта, в современном обществе является неотъемлемой частью деятельности в сфере исследования травм в сравнении с традиционными методами. В настоящем ведутся активные разработки развития сканирования в судебной медицине и создание аппаратуры, максимально отвечающей требованиям судебно-медицинских экспертиз, в частности, к таковым можно отнести технологии универсального сканирования (Universal Scanning Technology, UST). Существенный интерес здесь представляет возможность использования одного устройства как для сканирования мелких объектов (1 x 1 мм) до крупных (до нескольких метров) [3. С. 159]. Существенным усовершенствованием стала и возможность получения трехмерных моделей, воссоздаваемых на базе двухмерных изображений (таких как цифровые фотографии и видеозаписи).

Актуальной проблемой для медико-криминалистических экспертов является идентификация групповых и индивидуальных признаков орудия травмы по морфологическим особенностям повреждений, включая идентификацию личности с помощью скелетных останков. Отчасти существующие проблемы объясняются небольшим размером тела, предоставленного на судебно-медицинскую экспертизу [9. С. 428]. Для идентификации личности существуют различные методы, а именно: пластическая реконструкция лица по черепу, а также совмещение пожизненной фотографии человека с фотографией его черепа. Такого рода метод называется фотосовмещением [2].

При изучении судебно-медицинским работником изображений, сделанных на месте преступления, крайне сложно оценить реальный ход событий. Эти трудности вызвали необходимость разработки и применения методики получения 3D-изображения трупа, путем его сканирования. Такая возможность детального изучения судебно-медицинских объектов на теле и одежде, существенно сокращает время, необходимое для выполнения данной задачи при использовании классических методов. То есть копия исследуемого объекта, особенно виртуальная, становится незаменимой для повторного исследования судебно-медицинским экспертом, особенно, если повторное использование первичного препарата невозможно.

Технология трехмерного сканирования также позволяет провести цифровую идентификацию. Выявление дефектов во внешних покровах и внутренних органах дает возможность теоретически смоделировать механизм получения той или иной травмы. Помимо этого, такого рода сканирование допускает оценивание открытых травм и дает расчет соотношения размера травмированного участка к общей поверхности тела, что облегчает работу специалиста в получении более точных данных и в значительной степени ускоряет ее.

В ходе судебных экспертиз необходимо решать и проводить требуемые эксперименты, включающие моделирование либо исследуемого события, либо определенного материального объекта. В судебной практике нередко можно встретить случаи острой потребности воссоздания картины места происшествия [7. С. 196].

Технология 3D-печати имеет широкое распространение в медицине, а также в судебной медицине. Данный вид технологического прогресса имеет существенное значение в вопросах протезирования недостающих и восстановления поврежденных участков тела. Первые случаи применения 3D-печать зафиксированы уже в 1990-х годах. Изначально применялся такой метод, как стереолитография (технология аддитивного производства из жидких фотополимерных смол моделей, прототипов и готовых изделий), которая в судебной медицине была впервые предложена С. С. Абрамовым в 1998 г. [1. С. 14]. Дальнейшие разработки позволили использовать стереолитографию при оценке механизма повреждения костей. В текущее время данная технология практически заменена на 3D-печать необходимых в практике судебно-медицинского эксперта недостающих частей скелета для реконструкции травм лица при их компенсации, особенно это необходимо после забора этих частей для дополнительных инструментальных и лабораторных исследований [8. С. 11].

Современные высокотехнологичные методы исследования в судебно-медицинской (и иной) судебной экспертизе активно применяются в экспертизе вещественных доказательств. Так, активно их используют: 1) при установлении (опровержении) биологического родства; 2) при молекулярно-генетической идентификации личности; 3) в ходе судебно-химического или химико-токсикологического анализа наркотических или токсических веществ; 4) особенно актуальны современные методы при проведении медико-криминалистических экспертиз по установлению (отождествлению) повреждений у потерпевшего и травмирующего орудия [4. С. 27]. Полагаем, необходимо учитывать значительный потенциал виртопсии (предсекционное КТ-исследование) для установления особенностей течения па-

тологических процессов у конкретного пациента без вскрытия тела усопшего, особенно при наличии значительного количества телесных повреждений, которые делают судебно-медицинскую экспертизу трупа, проводимую в обычном порядке, достаточно затруднительной, а в ряде случаев может способствовать злоупотреблениям со стороны патологоанатомов [5. С. 160–163]. В настоящее время виртопсия уже внедрена в танатологическую практику Бюро СМЭ ряда регионов Российской Федерации [4. С. 27].

Стоит упомянуть об основных преимуществах технологии 3D-печати. К таковым можно отнести в первую очередь элементы этического наполнения, так как становится возможным изъять отдельные кости (например, череп или тазовые кости) без существенного нарушения внешнего вида трупа для продолжения необходимых медико-криминалистических исследований. Присутствуют и значительные экологические преимущества, связанные с легкостью изготовления и хранения (пластиковые 3D-копии не требуют сложных условий для хранения, в отличие от натуральных препаратов), хорошая устойчивость к внешним механическим воздействиям, наглядность и т. п. Также существенным является экономический эффект, связанный с относительно низкой стоимостью 3D-печати. В свою очередь, трехмерная печать, как инструмент для подготовки высококвалифицированных сотрудников в сфере судебной медицины, также является преимуществом.

Заключение. Следует сказать, что 3D-технологии играют значительную роль в качественной работе судебно-медицинского специалиста. Это своего рода вспомогательный инструмент работника в проведении экспертизы, так как трехмерное моделирование позволяет посмотреть на происшествие под другим углом и провести профессиональную оценку тех значимых деталей, которые было невозможно обнаружить в виду различных обстоятельств. Также использование различных 3D-технологий в деятельности судебно-медицинских экспертов может способствовать исключению излишних повреждений тела погибшего, что снимает вопросы у его родственников относительно возможного надругательства над телом умершего [6. С. 376].

Полагаем, что нужно активно развивать как цифровизацию в целом, так и наиболее перспективные 3D-технологии, используемые в деятельности судебно-медицинских экспертов. В связи с тем, что технологический процесс с каждым годом развивается в различных направлениях, это наталкивает на дальнейшее изучение данной темы.

Список литературы

1. Абрамов С. С., Болдырева Н. Н., Евсеев А. В. О возможности применения метода лазерной стереолитографии в судебной медицине // Судебно-медицинская экспертиза. 1998. № 3. С. 13–17.
2. Герасимов М. М. Восстановление лица по черепу (современный и ископаемый человек). Москва: Изд-во АН СССР, 1955. 585 с.
3. Ерофеев С. В., Шишкин Ю. Ю., Федорова А. С. Актуальные направления применения 3D-технологий в судебной медицине // Судебная медицина. 2016. Т. 2, № 2. С. 159–160.

4. Клевно В. А., Чумакова Ю. В. Виртопсия – новый метод исследования в практике отечественной судебной медицины // Судебная медицина. 2019. № 5 (2). С. 27–31. DOI: <https://doi.org/10.19048/2411-8729-2019-5-2-27-31>

5. Латыпова Э. Ю. Преступления, совершаемые врачами – патологоанатомами, постановка проблемы // Проблемы противодействия преступности: опыт, современное состояние и пути решения: сборник материалов Всероссийской научно-практической конференции, посвященной памяти профессора В. А. Малюткина. Чебоксары: Изд-во ЧГУ, 2019. С. 160–168.

6. Латыпова Э. Ю., Субаев М. А., Гильманов Р. Э. О проблемах состава на другательства над телами умерших и местами их захоронения // Актуальные проблемы правового, экономического и социально-психологического знания: теория и практика: материалы IV Международной научно-практической конференции. В 3 т. Донецк, 2021. С. 373–377.

7. Мусина Р. Р. К вопросу об особенностях осмотра места происшествия при падении с высоты // Актуальные проблемы юриспруденции в современном мире: сборник статей по материалам VII Всероссийской научно-практ. Конференции / под ред. Н. М. Швецова, Н. В. Иванцовой. Йошкар-Ола, 2017. С. 196–201.

8. Фришгонс Я., Кислов М. А., Леонов С. В. Использование 3D-печати в судебной медицине // Судебная медицина. 2018. № 2. С. 10–12.

9. Шайдуллина М. Р. Особенности судебно-медицинской экспертизы трупов новорожденных // Тамбовские правовые чтения имени Ф. Н. Плевако: материалы IV Международной научно-практ. конференции. В 2 т. Тамбов: Изд-во ТГУ, 2020. С. 428–430.

Н. Ш. Бабаназаров,

преподаватель,

кафедра цифровой экономики,

Туркменский государственный институт экономики и управления

ТРУДОВЫЕ ОТНОШЕНИЯ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. В данной работе рассмотрен вопрос развития трудовых отношений в период роста технологий и инноваций, влияние технологий на развитие дистанционных рабочих мест и влияние нового типа рабочих мест на продуктивность компаний. Проведен системный анализ развития цифровых технологий в сфере занятости населения. Даны рекомендации по внедрению технологий в отрасль по найму работников и в поиске подходящих кадров.

Ключевые слова: цифровая экономика, финансы, технологии

LABOR RELATIONS IN THE CONTEXT OF DIGITAL TRANSFORMATION

Abstract. In this paper, the issue of the development of labor relations in the period of growth of technologies and innovations, the impact of technology on the development

of remote jobs and the impact of a new type of jobs on the productivity of companies were considered. A systematic and analytical analysis of the development of digital technologies in the field of employment has been carried out. Recommendations are given on the introduction of technologies in the industry for hiring workers and in finding suitable personnel.

Keywords: Digital economy, Finance, Technology

Нынешняя фаза цифровизации обусловлена сложными и разнообразными взаимосвязями между данными, объектами и платформами, что приводит к кластерному разрушению и иногда к размытому ощущению изменений. Он характеризуется появлением новых передовых производственных технологий, алгоритмов машинного обучения, повсеместно распространенных устройств, а также приложений и услуг, управляемых данными. Среди прочего эти инновации включают передовую робототехнику и производственные системы 4.0, облачные вычисления и приложения «как услуга», интернет вещей, более интеллектуальные системы диспетчерского управления и сбора данных, расширенное обнаружение данных и бизнес-аналитику, глобальные платформы управления цепочками поставок и программные решения [1. С. 28].

Такие события предполагают необходимость пересмотра того, как в настоящее время составляются бизнес-модели. Наряду с появлением вышеупомянутых технологий разрабатываются новые бизнес-модели, и некоторые из них лежат в основе роста «сетевых рынков» и платформенной экономики. Одной из важных характеристик новых бизнес-моделей является их способность получать экономическую ренту за счет коммерциализации ранее недостаточно или совсем не использованных ресурсов. Преобразуя нашу повседневную жизнь в полезные данные, взаимосвязанные устройства, алгоритмы машинного обучения и онлайн-приложения расширяют потенциал для создания и использования новых источников стоимости. В новых моделях оцифрованные данные становятся стратегическим ресурсом, а потребитель – производителем цифровых товаров [2. С. 19].

В академических и общественных кругах ведется много дискуссий и споров о разрушительном воздействии нынешнего этапа цифровизации. Уорхерст и Хант (2019 г.) перечисляют три аспекта цифровизации, которые меняют работу и, следовательно, рынки труда: цифровые машины с искусственным интеллектом (ИИ); цифровизация процессов, предлагающая расширенные возможности обработки, хранения и передачи информации; и использование цифровых сетей для координации экономических транзакций с помощью платформенных алгоритмов. Ожидается, что эти изменения будут проходить через рынки труда и практики тремя путями. Первый способ касается обстоятельств, при которых технологические инновации в форме автоматизации, работы машин и систем искусственного интеллекта. В частности, утверждается, что цифровые технологии используются преднамеренно и инструментально для формирования работы и трудовых отношений; например, через онлайн-платформы. Во-вторых, цифровизация ускорила рост рабочих мест в сфере услуг и информации, а также сокращение рабочих мест в сфере производства и поиска материальных благ. В-третьих, с меньшим количе-

ством трудовых договоров, обеспечивающих «стандартные трудовые отношения», имело место последующее распространение нестандартных форм занятости. Как уже отмечалось, каким бы ни был конкретный опыт работы с неустойчивой занятостью и какими бы ни были текущие обстоятельства, эти новые разработки приносят элемент незащищенности со значительными рисками для здоровья. Они широки по своим последствиям и влияют не только на задачи в самой рабочей среде, но и на то, как люди работают и где они работают. Хотя на сегодняшний день эти изменения, похоже, не привели к увеличению безработицы, они могут быть связаны с ростом неполной занятости [3. С. 80].

Технологические инновации встроены в часто не признанные социальные отношения. Таким образом, внедрение и влияние цифровизации – это социальный процесс, который предвещает внедрение технических инноваций. В целом работодатели и правительства используют возможности для восстановления работы с помощью технологических инноваций. Несмотря на то, что эти факторы занимают доминирующее положение, рабочие и профсоюзы также не бессильны; они могут использовать свою свободу действий для оспаривания и, таким образом, формирования процесса и результатов цифровизации [4. С. 1].

Цифровизация ставит перед рабочим движением старые и новые вызовы. С самого начала индустриализации профсоюзы и их предшественники вели переговоры о внедрении новых технологий на рабочем месте, уделяя особое внимание тому, как они вытесняют рабочие места, реорганизуют рабочий процесс и влияют на формирование заработной платы. Но волна преобразований XXI в. ставит перед рабочими новые задачи в том, как они организуются и представляют себя в платформенной экономике. Продолжающиеся дебаты о цифровизации вызвали новый интерес к тому, как социальные партнеры могут участвовать в диалоге по этим возникающим вопросам. В то время как большая часть литературы посвящена тому, как профсоюзы могут организовывать и представлять работников платформы [5. С. 91].

Список литературы

1. Асемоглу Д., Паскуаль Р. Автоматизация и новые задачи: как технологии вытесняют и восстанавливают труд // Журнал экономических перспектив, 2019. № 33 (2). С. 3–30.
2. Агравал А., Джошуа Г., Ави Г. Машины прогнозирования: простая экономика искусственного интеллекта. Бостон: Harvard Business Review Press, 2018.
3. Багаутдинова Н. Г., Никулин Р. А. Новые конкурентные преимущества в условиях цифровизации // Инновации. 2018. № 8. С. 80–83.
4. Минделл Д. А., Рейнольдс Э. Б. Работа будущего: формирование технологий и институтов. Массачусетс: Массачусетский технологический институт (MIT), 2019.
5. Баранов Д. Н. Социально-экономические последствия распространения цифровых технологий на рынке труда // Вестник Московского университета им. С. Ю. Витте. Серия 1: Экономика и управление. 2018. № 3 (26). С. 91–97.

Г. М. Балахонцев,

студент,

Московский государственный университет имени М. В. Ломоносова

ИНФОРМАТИЗАЦИЯ ВНУТРЕННЕГО ФИНАНСОВОГО КОНТРОЛЯ

Аннотация. Целью исследования является анализ влияния политики цифровизации на осуществление внутреннего финансового контроля. В статье проанализированы мероприятия по внедрению информационных технологий внутреннего государственного финансового контроля в Российской Федерации. Обоснованы преимущества перехода к новой парадигме финансового контроля и недостатки системы финансового контроля, закрепленной в Бюджетном кодексе Российской Федерации. Выработаны предложения по совершенствованию нормативно-правового регулирования внутреннего финансового контроля.

Ключевые слова: внутренний финансовый контроль, информатизация, автоматизация, риск-ориентированность, информационные системы, СМАРТ-контроль, методы финансового контроля

INFORMATIZATION OF THE INTERNAL FINANCIAL CONTROL

Abstract. The aim of the study is to analyze the impact of digitalization policy on the implementation of internal financial control. The article analyses measures on introduction of information technologies of internal state financial control in the Russian Federation. The article justifies advantages of transition to a new paradigm of financial control and shortcomings of the system of financial control, enshrined in the Budget Code of the Russian Federation. Proposals for improving the legal regulation of internal financial control have been elaborated.

Keywords: Internal financial control, Informatization, Automation, Risk orientation, Information systems, SMART control, Methods of financial control

Цели многих стратегий, а также государственных и ведомственных программ, направлены на формирование цифровой экономики и повышение эффективности государственного управления. Одним из способов достижения вышеуказанных целей является внедрение информационных технологий. На Московском финансовом форуме заместитель руководителя Федерального казначейства Исаев Эли Абубакарович сказал, что Постановление Правительства от 14.04.2022 № 655, запрещающее проводить внутренний государственный финансовый контроль (далее – ВГФК) до 1 января 2023 г., дает нам понять, что деятельность по финансовому контролю из-за ее последующего характера может быть отложена на определенный срок, а нагрузка на объект контроля не является положительным аспектом контрольной деятельности [5]. Следовательно, в нынешних реалиях вектор развития ВГФК направлен в сторону информатизации и снижения нагрузки на подконтрольную среду. Дальнейшее запланированное развитие применения информационных систем при осуществлении ВГФК требует появления новых методических и нормативных документов. Так, проблемы реформирования финансового контроля в сторону его

информатизации и нормативного закрепления этих изменений являются достаточно актуальными в наше время.

Если обратиться к стандарту внутреннего финансового контроля, закрепляющему принципы деятельности органов внутреннего финансового контроля, можно заметить, что данная деятельность должна осуществляться в соответствии с такими принципами, как принцип информатизации, автоматизации и риск-ориентированности [8]. Принцип информатизации предполагает, что необходимые для осуществления контроля документы уполномоченный орган должен получать из государственных информационных систем, к которым он имеет доступ. Принцип автоматизации направлен на применение информационных технологий на всех этапах контрольной деятельности для оптимизации однообразных управленческих процессов или для анализа большого массива данных. Принцип риск-ориентированности означает концентрацию усилий контрольных органов в отношении тех объектов контроля, деятельность которых с большой вероятностью может принести ущерб бюджетной системе. Само описание данных принципов в стандарте указывает на внедрение в контрольную деятельность информационных технологий. Если реализовать эти принципы в ВГФК, то мы непременно выйдем на необходимость применения информационных технологий. Так, принципы автоматизации и риск-ориентированности могут быть реализованы через создание автоматизированной системы анализа рисков, которая реализована в ГИИС «Электронный бюджет». Функционал инструмента анализа рисков в ГИИС «Электронный бюджет» сочетает в себе различные средства автоматизации, такие как machine learning или применение подключаемых модулей на различных языках программирования [2]. При всем этом объекты контроля также отбираются автоматизированными алгоритмами на основе сочетания критериев «существенность» и «вероятность», закрепленных стандартом внутреннего государственного контроля, устанавливающим правила планирования контрольных мероприятий. Далее мы рассмотрим реализацию принципа информатизации. В 2022 г. в ГИИС «Электронный бюджет» в подсистеме информационно-аналитического обеспечения (далее – ПИАО) появился инструмент «Паспорт объекта контроля», который будет применяться сотрудниками контрольно-ревизионного блока Федерального казначейства с 2023 г. Данный инструмент непосредственно направлен на информационное обеспечение ревизоров и содержит в себе такие данные, как сведения о руководителе, организации в других источниках, учредителе, предшественниках, лицевых счетах в федеральном казначействе и т. д. Сформированный паспорт объекта контроля содержит информацию, которую ревизор учитывает при осуществлении контрольных мероприятий, например, сведения о реорганизации, смене адреса или организационно-правовой формы [10]. Помимо всего прочего, ПИАО также взаимодействует с данными таких информационных систем, как ГИР БО (хранит в себе бухгалтерскую отчетность контролируемого лица), ЕФРСБ (содержит сведения о банкротстве объекта контроля). Соответственно, данные внешних информационных систем могут дать информацию, которая в дальнейшем может использоваться ревизорами при проведении проверки (например, информацию об изменении кредиторской задолженности, банкротстве лица). Помимо хранения информации, данный инструмент способен выполнять и некоторые аналитические

функции, например, в нем реализованы автоматические алгоритмы рейтингования объектов контроля по определенным показателям (качество внутреннего финансового аудита, финансового менеджмента, рейтинг по закупкам). На примере инструмента «Паспорт объекта контроля» мы видим, что его функционал и хранящиеся в нем данные позволяют ревизору сразу получить информацию о контролируемом лице для проведения контрольно-ревизионных мероприятий, поскольку следует только правильно задать параметры поиска в инструменте, а также просмотреть документы в иных системах (гиперссылки на них находятся в ПИАО). Поскольку нужная документация не запрашивается у объекта контроля, а находится в информационной системе, то ревизоры тратят меньше времени на поиск информации, что снижает нагрузку на подконтрольную среду за счет уменьшения запросов о предоставлении дополнительных документов.

Таким образом, на сегодняшний день информационные технологии, применяемые в практике органов ВГФК, позволяют перевести подготовительную стадию, а также само проведение контроля в электронный формат без лишнего воздействия на подконтрольную среду.

Давно устоявшиеся формы бюджетного контроля, закрепленные Бюджетным кодексом (проверка, ревизия и обследование), неприменимы к новым вызовам для органов внутреннего финансового контроля в условиях внедрения информационных технологий в их деятельность. Полностью автоматизированный риск-анализ, применяемый в практике контрольных органов, не закреплен как форма или метод бюджетного контроля в нормативно-правовых актах, однако применяется органами ВГФК на практике. На его основе формируется карта рисков нарушений бюджетного законодательства, а также создается план контрольных мероприятий. Стоит заметить, что постепенно происходит отказ от выездных проверок в пользу камеральных, благодаря информационным системам и риск-анализу, что дает возможность ревизору дистанционно оценить эффективность и законность деятельности объекта контроля. ГИС, используемые в деятельности органов внутреннего финансового контроля через хранящиеся в них данные об объектах контроля, фактически позволяют сформировать «цифровой образ» этого объекта, который будет анализироваться ревизорами. В таком случае постепенно будет уменьшаться необходимость в такой форме контроля, как выездная проверка и иных формах, требующих прямое взаимодействие ревизоров с объектами контроля. Сотрудниками органа внутреннего финансового контроля, а также ведомственным проектом Министерства финансов отмечается тенденция к возрастанию «дистанционных» форм (мониторинг) и методов финансового контроля с применением информационных технологий (финансово-бюджетный мониторинг и финансово-бюджетный рулинг) [4. С. 47]. Э. А. Исаев видит в информатизации внутреннего финансового контроля смену самой парадигмы финансового контроля, где применение информационных технологий обуславливает переход к мониторингу действий объекта контроля в режиме онлайн и минимизирует проверки в отношении контролируемых лиц [3. С. 49]. Хотя методы новой парадигмы ВГФК не имеют нормативного закрепления, но их применение в практике органов ВГФК показывает высокую результативность. Из доклада заместителя главы Контрольного управления го-

рода Москвы Ю. В. Урожаевой на Московском финансовом форуме следует, что реализация SMART-контроля показала следующие результаты: 1) предотвращение нарушений на этапе предварительного контроля увеличилось до 80 %; 2) на 93 % снижено количество мероприятий последующего финансового контроля за счет мероприятий предварительного контроля [5].

Исходя из всего вышесказанного, можно сделать вывод, что ныне действующая и закрепленная в Бюджетном кодексе система внутреннего финансового контроля, делающая упор на проведение проверок, теряет свою актуальность в условиях информатизации, чему способствуют следующие факторы:

1) появление новых форм и методов осуществления внутреннего финансового контроля с использованием информационных технологий повышает эффективность планирования и проведения контрольных мероприятий и переводит последующий финансовый контроль в контроль в режиме реального времени;

2) новая парадигма финансового контроля предполагает взаимодействие с «цифровым образом» объекта контроля, формируемым на основе информации, полученной из ГИС, тем самым минимизируя воздействие контролирующего органа на контролируемое лицо и вмешательство ревизоров в деятельность объекта контроля.

Несмотря на активную информатизацию финансового контроля, в настоящее время большинство из нововведений не получило должного нормативного закрепления. В первую очередь ни на уровне законов, ни на уровне подзаконных актов новые способы и формы внутреннего финансового контроля не закреплены. Статья 267.1 Бюджетного кодекса РФ до сих пор содержит три формы финансового контроля: проверку, ревизию и обследование [1]. Согласно п. 3 ст. 269.2 БК РФ, деятельность по внутреннему государственному финансовому контролю урегулирована одноименными стандартами.

С 2020 г. принято семь таких стандартов. Стандарт, закрепляющий принципы осуществления внутреннего финансового контроля, регулирует применение информационных технологий в контрольной деятельности через закрепление уже упомянутых принципов информатизации, автоматизации и риск-ориентированности [8]. Стандарт, закрепляющий планирование контрольных мероприятий, указывает на то, что сбор и анализ информации об объектах контроля осуществляется с помощью информационных технологий, ручным способом либо комбинированным способом [6]. Допущение сбора и анализа информации ручным способом в стандарте нарушает принцип автоматизации, который предполагает применение информационных технологий, автоматизирующих однотипные бизнес-процессы, либо используемых при анализе большого массива данных. Осуществление сбора и анализа информации об объектах контроля – это достаточно большой объем данных, если посмотреть на годовые планы контрольных мероприятий как на федеральном, так и на региональном уровне. Следовательно, допущение применения ручного анализа рисков и сбора информации об объектах контроля должно быть исключено из стандарта планирования контрольных мероприятий. Также данный стандарт вносит дополнительные требования к информационным системам контрольных органов. В частности, вводятся критерии «вероятности» и «существенности», определен список информации по определению значения каждого критерия,

а также категории рисков. Стоит отметить, что списки информации по каждому критерию рисков и самих категорий рисков являются открытыми, из-за чего создатели ГИС могут прописывать дополнительную информацию для более обоснованной оценки показателей риска при планировании мероприятий.

Далее рассмотрим стандарт по проведению контрольных мероприятий. В рамках процесса информатизации данный стандарт регулирует запросы сотрудников органа внутреннего финансового контроля о предоставлении доступа к информационным системам объекта контроля и иных государственных органов, а также закрепляет формы, в которых отправляются документы объекта контроля в цифровой форме [9]. В стандарте закреплены контрольные действия в виде осмотра, инвентаризации, наблюдения, пересчета и контрольного обмера. Закрепленные контрольные действия, применяемые при проверках, присущи действующей системе финансового контроля, закрепленной в Бюджетном кодексе и не связаны с применением информационных технологий и имеющихся информационных систем. Работу с информационными технологиями и информационными системами, в рамках контрольных действий, ревизоры осуществляют лишь в рамках документального изучения информации, бухгалтерских и иных отчетных и финансовых документах. Контрольные действия по фактическому изучению объекта контроля не предполагает применения информационных технологий и информационных систем, поскольку в стандарте их использование не предусмотрено. Данный стандарт следует дополнить новыми формами и методами осуществления финансового контроля в виде финансово-бюджетного рулинга, финансово-бюджетного мониторинга и управления рисками, внедрение которых закреплено в ведомственном проекте Министерства финансов по развитию SMART-контроля [4. С. 47].

Подобное дополнение позволит на уровне нормативно-правовых актов закрепить методологию новой парадигмы внутреннего финансового контроля, где акцент будет делаться на камеральные проверки, мониторинг и применение информационных технологий. Последний рассматриваемый стандарт устанавливает права и обязанности сотрудников органа финансового контроля и объектов контроля [7]. В частности, в стандарте закреплено право сотрудников органа внутреннего финансового контроля на получение необходимого доступа к информационным системам объекта контроля и иных органов государственной власти, а также коррелирующую с этим правом обязанность предоставления объектом контроля доступа к собственной информационной системе сотрудникам органа контроля.

Таким образом, действующее нормативно-правовое регулирование внутреннего государственного финансового контроля все еще закрепляет существующую в Бюджетном кодексе систему ВГФК, изредка адаптируя применение информационных технологий в контрольной деятельности. Нормативные акты, регулирующие осуществление внутреннего финансового контроля, необходимо дополнить новой методологией планирования и осуществления внутреннего финансового контроля, которые получили развитие при внедрении информационных технологий в контрольную деятельность и уже применяются органами ВГФК на практике.

В заключение хотелось бы отметить, что применение информационных технологий в сфере внутреннего государственного финансового контроля стало предпосылкой к смене методологии внутреннего финансового контроля. Практика использования информационных технологий демонстрирует повышение эффективности контрольных мероприятий, а также снижение нагрузки на подконтрольную среду, что несомненно может служить основанием смены парадигмы внутреннего финансового контроля, где упор будет сделан на проведение камеральных проверок, мониторинга, аналитических мероприятий и информационных систем. Существующее нормативно-правовое регулирование новых методов контрольной деятельности ограничивается закреплением принципов, предусматривающих внедрение информационных технологий, регламентацией применения рискориентированного подхода при планировании контрольной деятельности и наделением сотрудников органов ВГФК правом получения доступа к информационным системам контролируемых лиц. Однако, несмотря на применение информационных технологий в практике осуществления ВГФК, появившаяся методология до сих пор не имеет должного закрепления ни на уровне законодательства, ни на уровне подзаконных актов.

Список литературы

1. Бюджетный кодекс Российской Федерации от 31.07.1998 № 145-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_19702/ (дата обращения: 30.08.2022).
2. ГИИС «Электронный бюджет». Новые возможности и сервисы для регионов на едином портале бюджетной системы (ЕПБС) и в подсистеме информационно-аналитического обеспечения (ПИАО) // URL: <https://www.krista.ru/wp-content/uploads/2022/04/Баркова-М.В.-Криста.pdf> (дата обращения: 10.09.2022).
3. Исаев Э. А. Подходы к цифровизации контроля в финансово-бюджетной сфере // Бюджет. 2019. № 5. С. 48–50.
4. Кораблев М. Н., Пахомова М. С. Федеральные стандарты как основа методологической конструкции ВГ(М)ФК // Бюджет. 2021. № 10. С. 44–47.
5. Московский финансовый форум. URL: <https://mff.minfin.ru/news/namoskovskom-finansovom-forume-obsudili-osnovnye-prioritety-razvitiya-sistemy-smartkontrol/> (дата обращения: 12.09.2022).
6. Об утверждении федерального стандарта внутреннего государственного (муниципального) финансового контроля «Планирование проверок, ревизий и обследований»: Постановление Правительства РФ от 27.02.2020 № 208 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_346639/ (дата обращения: 30.08.2022).
7. Об утверждении федерального стандарта внутреннего государственного (муниципального) финансового контроля «Права и обязанности должностных лиц органов внутреннего государственного (муниципального) финансового контроля и объектов внутреннего государственного (муниципального) финансового контроля (их должностных лиц) при осуществлении внутреннего государственного (муниципального) финансового контроля»: Постановление Правительства РФ от 06.02.2020

№ 100 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_344924/ (дата обращения: 30.08.2022).

8. Об утверждении федерального стандарта внутреннего государственного (муниципального) финансового контроля «Принципы контрольной деятельности органов внутреннего государственного (муниципального) финансового контроля»: Постановление Правительства РФ от 06.02.2020 № 95 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_344861/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/ (дата обращения: 30.08.2022).

9. Об утверждении федерального стандарта внутреннего государственного (муниципального) финансового контроля «Проведение проверок, ревизий и обследований и оформление их результатов»: Постановление Правительства РФ от 17.08.2020 № 1235 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_360482/ (дата обращения: 30.08.2022).

10. Руководство работников (представителей) участников системы «Электронный бюджет» по работе с подсистемой (компонентом, модулем) системы «Электронный бюджет». Государственная интегрированная информационная система управления общественными финансами «Электронный бюджет». Подсистема информационно-аналитического обеспечения. URL: <https://roskazna.gov.ru/gis/ehlektronnyj-byudzhjet/podsistema-informatsionno-analiticheskogo-obespecheniya/> (дата обращения 09.08.2022).

Э. Р. Бурангулов,

кандидат политических наук, доцент,

Уфимский государственный нефтяной технический университет

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ВЫСШЕМ ОБРАЗОВАНИИ РОССИИ: ПРОБЛЕМЫ В СФЕРЕ ИНТЕЛЛЕКТУАЛЬНОГО ПРАВА

Аннотация. В статье при помощи системного, неинституционального, сравнительного анализа выделяются основные пробелы в сфере интеллектуального права, возникающие при использовании цифровых технологий в высшем образовании России, предлагаются пути их решения. Делается вывод о том, что следует разработать правовые механизмы (нормативные правовые акты), которые обеспечивают защиту и поддержку социально ответственного применения цифровых технологий в сфере высшего образования, гарантируют электронные доступ к знаниям и новой информации для широких слоев общественности, особенно для малообеспеченных граждан.

Ключевые слова: высшее образование, дистанционное образование, предпринимательский университет, право, цифровые технологии

DIGITAL TECHNOLOGIES IN HIGHER EDUCATION IN RUSSIA: PROBLEMS IN THE FIELD OF INTELLECTUAL PROPERTY LAW

Abstract. The article highlights the main legal conflicts arising from the use of digital technologies in higher education in Russia using the materials of the author's research with the help of a systematic, neoinstitutional, comparative analysis.

It is concluded that it is necessary to develop legal mechanisms (regulatory legal acts) that protect and support the socially responsible use of digital technologies in higher education, guarantee electronic access to knowledge and new information for the general public, especially for low-income citizens.

Keywords: Higher education, Law, Digital technologies, Distance education

Введение. В последнее время расширяется и ускоряется процесс использования цифровых технологий в высшем образовании России: многофункциональных интернет-платформ обучения («Университет без границ», Moodle, iSpring); онлайн-инструментов (Kahoot, Buncee, Quizizz), виртуальных досок (MIRO, Twiddla, Scribblar) и др.

Происходящие процессы приводят к тому, что в сфере образования акценты смещаются с постепенного воспитания разносторонне развитой личности на ускоренную подготовку квалифицированного исполнителя, максимально востребованного в цифровой экономике знания.

Основная часть. Изменения в образовании, происходящие в рамках цифровой трансформации, можно оценивать в двух аспектах. Негативная сторона замечена многими еще в 1980-е гг. Так, ставка на извлечение прибыли становится причиной подчинения образовательных учреждений обладателям крупного капитала и их экономическим потребностям в ущерб ориентации на общественный прогресс и свободный поиск нового знания. Вследствие коммерциализации (одновременно с наступлением государства на свободу и приватность) сужается доступ к качественной информации, расширяется контроль и наблюдение, а также использование разного рода манипуляций в Интернете, что приводит к сжатию публичного пространства и области ценной, доступной и достоверной информации.

Иная сторона здесь – позитивная. Цифровая коммуникация в высшем образовании в виде электронного обучения и дистанционных технологий дает возможность экспортировать образовательные услуги на новые рынки, расширить круг потребителей (обучающихся), а также сократить текущие издержки, что приносит все больший доход.

Тенденция коммерческой цифровизации образования санкционируется идеями «академического капитализма» и «предпринимательского университета», определяющими то, что путевка в жизнь выдается только тем учебным курсам и научным исследованиям, которые отвечают критериям экономической результативности, перспективны для инвестиций, фондрайзинга [1].

Среди наиболее значимых сюжетов применения цифровых технологий в высшем образовании выделяются следующие:

- концентрация и удержание внимания студентов на онлайн-занятии;
- работа на многофункциональных интернет-платформах обучения («Университет без границ», Moodle, iSpring, WebTutor, Teachbase, GetCourse, Memberlux);
- использование онлайн-инструментов (Kahoot, Buncee, Quizizz, Padlet, My simple show, Peardeck, Labster, Istation), виртуальных досок (MIRO, Twiddla, Scribblar).

- постановка онлайн-занятия, методики его проведения;
- правовые коллизии и др.

Среди правовых коллизий особенно необходимо отметить проблему интеллектуального (авторского) права в цифровой среде. Например, в тех случаях, когда онлайн-лекции записываются и распространяются без разрешения преподавателя или, более того, обнародуются под чужими фамилиями.

Также стоит отметить проблему шифрования данных с масштабным применением процедур аутентификации под именем борьбы за безопасность (со стороны государства) и под лозунгом защиты авторских прав (со стороны корпораций). Под указанными благовидными предложениями, на наш взгляд, осуществляется ущемление прав граждан на свободу, приватность, возможность получить нужные сведения для добросовестного личного некоммерческого использования (самостоятельных научных исследований). Мы ни в коем случае не посягаем на священные права авторства, лишь хотим заметить, что на современном технологическом уровне можно соблюсти благоразумный баланс между коммерческим и некоммерческим благонамеренным использованием результатов научных исследований, избежав при этом опасности плагиата. Большое подспорье в этом направлении может оказать создание свободной базы данных исследований с указанием первоначального авторства, а также использование программного обеспечения с открытыми исходными кодами.

Заключение. В настоящее время применение цифровых технологий в высшем образовании России все более заметно уклоняется в сторону извлечения прибыли. Разработка и внедрение новых инструментов делается не столько для расширения доступа широкой аудитории к знаниям и новой информации, для общественной пользы, сколько для увеличения числа потребителей платных продуктов, производимых вузами, все более напоминающими коммерческие корпорации. Вместе с тем представляется перспективным, чтобы скорректировать текущий процесс использования цифровых образовательных технологий так, чтобы некоторая сумма полученных доходов по принципу социальной ответственности и согласно справедливому механизму перераспределялась на развитие тех направлений, которые требуют затрат и не дают быстрого коммерческого эффекта (фундаментальные исследования, обучение студентов из малообеспеченных семей и т. д.). Для этого членам образовательного сообщества необходимо более громко заявлять о классической миссии университета и о большом значении долгосрочной стратегии общественного развития, которые, кстати, также приносят свои плоды в виде нематериальных активов. В этой связи следует разработать правовые механизмы (нормативные правовые акты), которые обеспечивают защиту и поддержку социально ответственного применения цифровых технологий в сфере высшего образования, гарантируют электронный доступ к знаниям и новой информации для широких слоев общественности, особенно для малообеспеченных граждан.

Список литературы

1. Руткевич А. Три идеи университета // Вопросы философии. 2022. № 7. С. 66–74.

Д. С. Вебер,

студент,

Томский государственный университет
систем управления и радиоэлектроники

С. Р. Гадельшина,

студент,

Томский государственный университет
систем управления и радиоэлектроники

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ CRM-СИСТЕМЫ

Аннотация. На сегодняшний день человечество живет на таком этапе общественного развития, на котором главную ценность играет информация, что повышает важность сохранения ее конфиденциальности и ограничение доступа к ней. CRM-система является колоссальным источником такой информации, чтобы минимизировать риски, владельцу конфиденциальной информации необходимо придерживаться и соблюдать все способы защиты, которые помогут избежать незаконного получения данных и в некоторых случаях восстановить нарушенные права. Целью доклада является определение типичных ошибок при защите конфиденциальной информации при использовании автоматизированной системы.

Ключевые слова: CRM-система, конфиденциальная информация, защита информации, режим коммерческой тайны, соглашение о неразглашении, персональные данные, коммерческая тайна

PROTECTION OF CONFIDENTIAL INFORMATION WHEN USING THE SYSTEM

Abstract. Today, humanity lives at a stage of social development where information plays the main value, which increases the importance of maintaining its confidentiality and restricting access to it. The CRM system is a huge source of such information, in order to minimize risks, the owner of confidential information in the CRM system must adhere to and comply with all methods of protection that will help avoid illegal data acquisition and, in some cases, restore violated rights. The purpose of the report is to identify typical errors in the protection of confidential information when using an automated system. The purpose of the report is to identify typical errors in the protection of confidential information when using an automated system.

Keywords: CRM-system, Confidential information, Information protection, Trade secret regime, Trade secret, Non-disclosure agreement, Personal data

Важным элементом многих современных предприятий является CRM-система. Цифровые технологии не стоят на месте, а одним из первостепенных факторов успеха предстает эффективная автоматизация всех его внутренних процессов.

Нынешняя экономика создает ситуации, в которых необходимо непрерывно повышать эффективность производства, оперативно реагировать на внезапные

трансформации, в том числе в законодательстве, улучшать уровень обслуживания, сокращать потери, выстраивать эффективные прогнозы, а также обезопасить себя от утечки данных, а как следствие, от связанных с этим рисков. Поэтому руководителю компании следует обладать надежными сведениями для аналитического исследования функционирования фирмы в реальном времени. Именно для этого многие фирмы так активно внедряют автоматизированные системы. Особенно это актуально для новых компаний, деятельность которых связана с IT-технологиями.

Информационные технологии, которые достигли в минувшие годы значительно более качественной и высокой степени развития, стабильно увеличивают показатели эффективности и предоставляют все более новые способы обработки и анализа экономической информации, необходимой для стратегического принятия решений.

Под CRM-системой понимают автоматизированную систему, ориентированную на быстрое рекрутирование, сопровождение и удержание клиента с целью настоящего и последующего сотрудничества [2. С. 204]. Система грамотно систематизирует полученную информацию и хранит базе.

CRM-система способствует хранению всей истории взаимоотношений с клиентами в одном месте и данные находятся в доступе сотрудников.

Все CRM-системы включают в себя такие элементы, как:

- Управление контактами;
- Управление продажами;
- Управление электронной торговлей [1. С. 179] и т. д.

CRM-система хранит персональные данные, поэтому необходимо защитить их от разглашения. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)» [5]. К примеру, ФИО, номер телефона и т. п.

Соглашения о неразглашении, которые подписывают компании, едва ли способны обезопасить конфиденциальную информацию. Проблема в том, что для защиты информации необходимо соблюсти требования, на которые обращают внимание далеко не все.

Для того чтобы разобраться в том, почему так происходит, необходимо понимать и разграничивать понятия конфиденциальной информации и информации, которая содержит коммерческую тайну. Второе включает сведения в том числе о результатах интеллектуальной деятельности, а также о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа и в отношении которых обладателем таких сведений введен режим коммерческой тайны [6].

Если посторонним открывается доступ к такой информации, то она теряет свою значимость. Например, информация о технологиях, используемая в организации или компании, составляет информацию, содержащую коммерческую тайну, поскольку, став известной конкурентам, ее ценность значительно снизится. Однако, например, информация о том, сколько денежных средств находится в распоряжении организации и с какими клиентами она сотрудничает, не может составлять коммер-

ческую тайну, поскольку разглашение такой информации не обесценивает ее, но тем не менее не отменяет возможность убытков. Эту информацию можно и нужно защищать, однако она относится уже к категории конфиденциальной информации. В нее включается вся информация, относительно которой сторонами был достигнут консенсус, например о данных в CRM-системах.

Подобное деление крайне важно учитывать, потому что если компания определяет информацию о балансе своего счета или данные о работе с клиентами как коммерческую тайну, то, вероятнее всего, в случае судебного спора суд может не признать в качестве нарушения ее разглашение. Более того, в соглашении о неразглашении всегда нужно конкретно, четко и развернуто описать ту информацию, которую нельзя разглашать. Не должны применяться абстрактные формулировки, иначе в случае разглашения привлечь к ответственности будет крайне сложно.

Например, в постановлении суда было принято решение отказать истцу в удовлетворении требований, так как в договоре не было указано списка конфиденциальной информации: «В этой связи суд первой инстанции обоснованно пришел к выводу о том, что ввиду отсутствия в договоре и соглашении указаний на конкретный перечень сведений, в отношении которых может быть установлен режим коммерческой тайны, ответчиком не доказан факт нарушения истцом данного режима» [4].

Поэтому обязательно необходимо составлять полный список отдельным приложением к соглашению о неразглашении. Более того, нужно показать, что информация относится к конфиденциальной.

Распространенной проблемой при подготовке и подписании соглашения о неразглашении также является несоблюдение императива Закона «О коммерческой тайне». Он содержит меры по охране такой информации, который ее обладатель обязан принять. Например, составить перечень информации, составляющей коммерческую тайну и ограничить доступ к такой информации, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка [6].

Чтобы был соблюден последний пункт, необходимо прописать в соглашении точный порядок обращения с информацией: как ее следует хранить, как передавать и т. д. – в противном случае суд, вероятнее всего, признает отсутствие введения режима коммерческой тайны в организации, и даже в случае доказанного нарушения взыскать ничего не удастся.

В случае наличия работников можно было бы установить определенный порядок обращения с информацией. Принятие внутреннего Положения о конфиденциальности разрешило бы этот вопрос.

Например, в одном из постановлений Арбитражного суда был рассмотрен спор по иску предприятия, работник которого открыл ИП, а при увольнении взял из базы данные о клиентах этой компании с целью привлечения к себе на более выгодных условиях. Даже с учетом того, что истец привел доказательства, которыми в том числе выступали сами клиенты, суд решил отказать в иске из-за того, что сам истец не посчитал нужным вводить в компании режим коммерческой тайны и не учел требований статей Закона «О коммерческой тайне» [3].

Итак, соглашения о неразглашении бывают несколько видов:

– не работающие с самого начала (те, что сразу будут признаны незаключенными);

- формальные (с которыми с нарушителя ничего взыскать не получится);
- нормальные (в которых приняты все меры по введению конфиденциальности).

Таким образом, использование CRM-систем будет актуальным и перспективным вложением компании. Для того чтобы в действительности защитить конфиденциальную информацию и иметь возможность привлечь виновного в ее разглашении к ответственности, следует подойти к этому вопросу крайне серьезно. Для того чтобы исключить утечку информации, необходимо разграничить доступ к системе согласно функциональным возможностям работников компании. Необходимо внимательно рассматривать ситуацию и подготавливать документы, следуя положениям закона и руководствуясь судебной практикой. Иначе последствия могут быть не самыми удачными, поскольку автоматизированная система обладает огромным количеством информации, что в информационном мире имеет принципиальное значение.

Список литературы

1. Ключкова А. В., Бебякина А. А. CRM-система как инновационный инструмент повышения конкурентоспособности организации // Экономика и экологический менеджмент. 2019. № 4. С. 177–184.
2. Костенко Е. А., Усенко Р. С. Современные тенденции развития CRM-систем // Теория и практика экономики и предпринимательства: науч. сборник. 2020. С. 204–205.
3. Постановление Арбитражного суда Поволжского округа от 10.07.2012 А57-11021/2011 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=APV&n=102983#OvR_6cHTqesgOE_7ND_1.
4. Постановление Тринадцатого арбитражного апелляционного суда от 03.07.2015 г. А56-72074/2014 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=RAPS_013&n=170948#MAP2cHTtsthkLsA.
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3451.
6. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // Собрание законодательства РФ. 09.08.2004. № 32. Ст. 3283.

Т. В. Вербицкая,

кандидат политических наук,
преподаватель Уральского федерального университета,
научный сотрудник Государственного архива Свердловской области

ЦИФРОВЫЕ КОПИИ ПРАВОВЫХ АКТОВ XVIII-XX ВЕКОВ ДЛЯ ИЗУЧЕНИЯ ИСТОРИИ ПРАВА (НА ПРИМЕРЕ ОПЫТА СОЗДАНИЯ И ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОГО ПОРТАЛА О ПРОМЫШЛЕННИКАХ ДЕМИДОВЫХ)

Аннотация. Актуальность исследования обусловлена тем, что цифровые технологии, применение которых является неотъемлемым элементом большинства сфер жизни государства и общества, в том числе и юриспруденции, могут

быть действительно использованы и в тех областях, для которых подобные современные технологии не представлялись необходимыми: при изучении истории права. Поскольку правовые акты разных эпох находятся на хранении в разных архивах, то систематизированное их изучение возможно только, если будут создаваться межархивные коллекции цифровых копий таких правовых актов с внедрением возможности поиска по разным атрибутам. Опыт создания, развития, наполнения сайта по истории рода заводчиков и государственных деятелей Демидовых коллекциями правовых актов XVIII–XX вв., составленных в отношении разных представителей указанной династии, позволяет определить, что цифровые технологии могут быть успешно внедрены и для изучения истории права. В результате проведенного исследования автор приходит к выводу, что создание подобных информационных порталов с коллекциями цифровых копий документов будет способствовать комплексному, систематизированному подходу к изучению особенностей эволюции разных феноменов в сфере юриспруденции.

Ключевые слова: оцифровка, история права, коллекции документов, информационный ресурс, портал, правовой акт

DIGITAL COPIES OF LEGAL ACTS OF THE XVIII-XX CENTURIES FOR THE STUDY OF THE HISTORY OF LAW (ON THE EXAMPLE OF THE EXPERIENCE OF CREATING AND FUNCTIONING OF THE INFORMATION PORTAL ABOUT INDUSTRIALISTS DEMIDOV)

Abstract. The relevance of the study is due to the fact that digital technologies are integral element of most spheres of state and society existence, including jurisprudence and can be effectively used in areas for which such modern technologies did not seem necessary: the history of law. Since law acts of different eras are stored in many archives, their systematized study is only possible if inter-archival collections of digital copies of such law acts are created with the introduction of the ability to search by different attributes. The experience of creating, developing, filling a site on the history of the family of breeders and statesmen Demidoffs with collections of law acts of the 18th-20th centuries, in correlation with various representatives of this dynasty, allows us to determine that digital technologies can be successfully introduced to study the history of law. The author comes to the conclusion that the creation of such information portals with collections of digital copies of documents will contribute to a comprehensive, systematic approach to studying the evolution of various phenomena in the field of jurisprudence.

Keywords: Digitization, History of law, Collections of documents, Information resource, Portal, Law act

Цифровые технологии являются неотъемлемым элементом всех сфер жизни общества в государстве, так, что происходит процесс взаимного обогащения и совершенствования: по мере развития общества и элементов системы государственного управления, развиваются и цифровые технологии в качестве необходимых инструментов профессиональной жизни, политического и правового регулирования. Так, все задачи, проблемы, требующие внимания и быстрого реагирования,

оперативно решаются, поскольку цифровые ресурсы позволяют с учетом заданных параметров найти наиболее оптимальное решение. Кроме того, все более часто и успешно указанные современные технологии используются в областях, по времени отдаленных от современной жизни, например, при изучении правовых процессов предшествующих эпох. Современные подходы в науке требуют комплексности, т. е. при анализе какой-либо проблемы, нужно ее изучить посредством целой совокупности методов и инструментов, что особенно актуально при анализе отдельных явлений и процессов в сфере права при регулировании общественных отношений в исторической перспективе. Цифровые технологии содействуют тому, чтобы такая комплексность в исследовании была обеспечена, поскольку с их помощью можно объединить правовые акты разных периодов в коллекции по разным критериям в одной или нескольких информационных системах и обеспечить возможность поиска интересующих документов по атрибутам. Опыт создания и функционирования сайта по истории рода государственных и промышленных деятелей Демидовых (<https://демидовы.рус>), на котором размещены цифровые копии правовых актов (судебные решения, договоры, расписки, завещания), составленных в периоды XVIII–XX вв. в отношении разных представителей данного рода, их доверенными лицами позволяет оценить значимость информационных технологий при изучении особенностей развития отдельных правовых явлений и процессов на конкретных практических кейсах.

Наполнение контентом информационного портала, посвященного роду горных промышленников и государственных деятелей Урала и всей России – Демидовых – происходило посредством развития диалога архивов России и зарубежных стран (в первую очередь Франции и Италии) в рамках обмена документами по истории рода Демидовых. Актуальность создания и наполнения правовыми актами информационного портала по истории именно заводчиков Демидовых, состоит во-первых, в силу того, что потомки Демидовых живут во Франции, Италии, Великобритании и Греции, и контакты с ними по вопросам изучения документов по истории рода Демидовых позволит наладить диалог с соотечественниками за рубежом, во-вторых, информационный портал, полученный в итоге изучения, анализа, перевода с французского, итальянского языков полезен в исследовательских целях, поскольку позволяет через призму документов, составленных Демидовыми и их представителями составить представление об особенностях деловой жизни в России и Западной Европы в XVIII–XX вв., в-третьих, представление достижений Демидовых в благотворительности, коллекционировании, развитии науки и искусств как элемента исторического наследия России и Свердловской области позволит развивать имидж Свердловской области и тем самым укреплять ее связи с партнерами внутри страны и за ее пределами и налаживать новые.

Полученный портал как результат межархивного взаимодействия, предметом которого являлись Демидовы как государственные и общественные деятели Урала, России, известные в Италии, Франции и Италии позволит развивать сотрудничество по правовым вопросам и в сфере архивного дела посредством демонстрации уже полученных в рамках межархивного взаимодействия результатов и представить для потенциальных партнеров России продукт, который может за-

интересовать их. Кроме того, такое представление культурного наследия позволяет развивать и в дальнейшем имидж и Свердловской области внутри России и за ее пределами.

Так, размещенные на сайте <https://демидовы.рус> материалы позволяют установить, что колыбелью Демидовых как виднейшей общероссийской династии горнозаводчиков, государственных и общественных деятелей, меценатов, коллекционеров является Урал. Нижнетагильский завод всегда воспринимался ими как оплот их благосостояния. С 1720 г. благодаря развитию горного дела на Урале и за его пределами Демидовы получили дворянство, кроме того, постепенно они стали расширять торговлю железом и другими металлами за пределы Российской Империи, используя свой торговый знак, получивший название «Древний соболь», ставший известным на рынках металлов Италии, Англии и Франции. В знак признания их заслуг в качестве исторического наследия, ключевым элементом современного герба Свердловской области выступает соболь.

Огромное значение имеет вклад Демидовых в развитие науки. Широкого известна вручаемая и в настоящее время премия Демидовых. Начиная от Акинфия Никитича Демидова, представители этого рода жертвовали на открытие школ, учреждений общественного призрения, высших учебных заведений (включая МГУ) в России и за ее пределами (так, в городе Сан Никкола Николай Никитич Демидов открыл школу совместного обучения, при которой были теплицы, мастерские, термы), финансировали обучение талантливых россиян разным ремеслам и искусствам. И информационный портал по истории рода Демидовых подтверждает то, что Демидовы являлись выдающимися российскими меценатами – на портале размещена скан-копия распоряжения Анатолия Николаевича Демидова в Санкт-Петербургскую заводскую контору о ежемесячном выделении денежной суммы для оказания помощи бедным от 26 марта 1830 г. [1. Д. 208. Л. 38], акта от мая 1829 об учреждении банного комплекса для бедных в Линце, Австрии на основании пожертвований Н. Н. Демидова [1. Д. 221. Л. 42]; письмо от 26 мая 1856 г. А. Н. Демидова В. А. Долгорукову о пожертвовании 600 тыс. рублей на военные нужды, связанные с ведением Крымской войны [1. Д. 385. Л. 14] и много других документов, которые позволяют убедиться в масштабах деятельности Демидовых в качестве благотворителей.

Правовые акты на сайте <https://демидовы.рус> позволяют убедиться, что благодаря своей деятельности на дипломатическом поприще, участию в развитии международного гуманитарного права в рамках помощи военнопленным, раненым и больным в действующих армиях (немалый вклад на этом поприще внес Анатолий Николаевич Демидов) [6. С. 421] и международной торговле Демидовы становятся известными во Франции и Италии, и начинают активно участвовать в политической жизни этих стран [5. С. 172]. За свои заслуги Павел и Анатолий Николаевичи Демидовы стали кавалерами Легиона чести во Франции; начиная с Анатолия Николаевича, Демидовым стал также присваиваться титул «князь Сан-Донато» [3. Л. 4].

Поскольку Демидовы имели резиденции в Санкт-Петербурге, Нижнем Тагиле, во Флоренции (Сан-Донато) и в Париже, то составленные ими документы хранятся

в архивах России, Франции и Италии. В силу роли и значения Демидовых в этих странах, сбор, перевод, анализ, изучение документов (деловых писем, договоров, расписок, актов) позволяет составить представление о жизни и деятельности этих ведущих государственных и общественных деятелей как историческом наследии России в целом и Урала в частности. Кроме того, поскольку, начиная с первой четверти XIX в. Демидовы постоянно проживали за рубежом России [3. С. 101], изучение истории этого рода возможно благодаря общению с живущими в настоящее время представителями рода Демидовых.

Именно поэтому создание и наполнение контентом сайта по истории рода Демидовых происходило посредством реализации ряда этапов: 1) деловые поездки в архивы Франции, Италии (на протяжении 2018–2020 гг.), а также в архивы России (в Москве, Санкт-Петербурге, Алтае, Нижнем Новгороде) в целях сбора и анализа хранящихся там документов по истории рода Демидовых и налаживание контактов с представителями этих архивов для создания основ межархивного взаимодействия; 2) перевод полученных документов и их классификация по критериям: государственная, общественная жизнь Демидовых, коллекционирование, документы, посвященные вопросам владения Демидовыми имений в России и за рубежом; 3) разработка концепции информационного портала по истории рода Демидовых (кроме документов, составленных на французском и итальянском языках, которые размещены на портале с переводом на русский язык и с метаданными, на сайте представлены аналитические материалы, в том числе статьи сотрудников Государственного архива Свердловской области, составленные по итогам изучения полученных архивных документов); 4) наполнение информационного портала по истории рода Демидовых контентом; 5) популяризация портала посредством проведения выставок документов (в период с 8 сентября по 3 октября 2021 г. был реализован Международный выставочный проект «Первые Демидовы: Рождение горнозаводской империи»); 6) налаживание благодаря этим мероприятиям диалога с потомками Демидовых, которые в настоящее время проживают в Италии, Франции и Великобритании.

Как было указано, правовые акты, размещенные на сайте по истории рода Демидовых, можно классифицировать: 1) по сфере, в которой акт был принят, и выделить акты о профессиональной деятельности (инструкции, грамоты о присвоении дворянства, формулярные списки, послужные списки, служебные паспорта); документы личного характера (завещания, акты о рождении, заключении брака, смерти), имущественные (купчая, договоры купли-продажи, акты о разделе имущества, квитанции, расписки) и документы, принятые по вопросам благотворительности (дарственные, учредительные документы благотворительных учреждений); 2) по периодам в связи с личностью представителя рода Демидовых, жившим в этот период: XVIII в. – основатель рода Демидовых (Никита Антуфьев Демидов), Демидовы-уральские заводчики (Акинфий Никитич Демидов и его сыновья Прокопий, Никита и Григорий); XIX в. – флорентийская ветвь Демидовых как государственных, промышленных и общественных деятелей – Николай Никитич Демидов, его сыновья Анатолий и Павел и внук, Павел Павлович Демидов; XX в. – Демидовы-дипломаты – сыновья Павла Павловича Демидова.

Подобный информационный портал представляет собой интерес именно благодаря своей эмпирической направленности, поскольку позволяет соотнести контекст периода, в который он был принят, события из жизни определенного представителя рода Демидовых, жившего в этот период и специфику содержания правового акта, принятого с учетом правоприменительной практики и обычаев делового оборота этого периода и действовавших в то время нормативно правовых актов. В связи с изложенным представляется необходимым привести пример того, как применяется личный закон в качестве элемента международного частного права во Франции в первой четверти XIX в. по делу Деспан (все цифровые копии документов по этому делу размещены на сайте <https://демидовы.рус>). Так, в августе 1827 г. воспитанница Николая Никитича Демидова по фамилии Деспан подала в суд в Париже заявление о признании его отцовства. Поскольку в 1828 г. Николай Никитич Демидов умирает, то судебный процесс завершается с участием сыновей Н. Н. Демидова Павла и Анатолия и принимается решение о неподсудности суду Франции дела о признании отцовства в отношении российского подданного [1. Д. 176. Л. 2–2 об; Д. 188. Л. 59–64]. Кроме того, муж заявительницы Деспан стал советником при дворе Российской Империи и таким образом утратил качества гражданина Франции [1. Д. 188. Л. 79–79 об].

Особенностью данного портала является удобный поиск по атрибутам: году принятия, ключевым словам, архиву, в котором содержится данный документ, персоналии (представителю рода Демидовых), в отношении которого принят данный акт; также возможен поиск, по ключевым словам, заголовке непосредственно по списку документов (вкладка «Документы»). Помогает при осуществлении поиска обращение к разделам «Вид документа» (в том числе договор, рескрипт, расписка, решение, купчая, завещание), «Автор документа», «Адресат» (поскольку к каждой персоналии и государственному и общественному учреждению привязаны документы, в отношении которых они были приняты), словарю персоналий. Также систематизированное изучение интересных документов возможно посредством обращения к вкладке «Коллекции документов», в которых правовые акты объединены по объекту – например, имениям Демидовых в России и за рубежом (договоры купли-продажи имения Сан-Донато, Пратолино, дачи Често, аренды дворца Серристоры), благотворительности (учредительные документы благотворительных учреждений, основанных Демидовых), торговле металлами (договоры), финансовым операциям (расписки), ремонтным работам (договоры и акты выполненных работ), морским перевозкам (погрузочные квитанции), государственной службе (формулярные списки).

К числу функций такого информационного ресурса, как портал по истории рода Демидовых, на котором размещены коллекции правовых актов, можно отнести:

1) интегрирующую – ресурс объединяет в себе материалы и документы, позволяющие узнать об особенностях эпохи в целом, факты из жизни тех, в отношении кого составлялись правовые акты, т. е. изучить контекст, особенности сферы регулирования посредством указанных правовых актов;

2) систематизирующую – формируются коллекции документов по разным критериям: времени, месту создания, особенностям сферы регулирования (госу-

дарственная служба, предпринимательская, промышленная деятельность, благотворительность), субъекту (представителю рода Демидовых, в отношении которого был составлен документ) и виду правового акта;

3) познавательную – информационный ресурс позволяет получить в структурированном виде интересующие сведения;

4) накопительную – объединяет правовые документы, коллекции которых постоянно пополняются и могут быть дополнены по мере подготовки цифровых копий таких документов;

5) развивающую – позволяет дополнять деталями и углублять представление как об особенностях правового регулирования, так и специфике регулируемых общественных отношений и жизни представителей рода Демидовых в разные исторические периоды;

6) эмпирическую – с его помощью возможно соотнести особенности принятых правовых актов со спецификой ситуации, в контексте которой они были приняты.

Исходя из изложенного, опыт функционирования такого сайта позволяет оценить полезность сохранения и развития данной практики по функционированию информационных порталов, посвященных выдающимся государственным и общественным деятелям (которыми очень богата Россия), содержащим в себе как правовые акты и документы, так и иные материалы по фактам биографии такого деятеля и характеристики эпохи: ученым (например, М. В. Ломоносов), государственным деятелям (в качестве примера можно привести М. М. Сперанского), в том числе дипломатам (например, А. М. Горчаков).

Таким образом, цифровые технологии являются ресурсом, позволяющим реализовать комплексный подход к изучению истории права, выполняя две функции: формирование коллекции правовых актов разных периодов, их объединение с соблюдением требования единообразия; систематизация правовых актов по различным критериям, с предоставлением возможности осуществления поиска по атрибутам. В силу того, что правовые акты нескольких веков, относящиеся к разным историческим событиям, лицам, территориям, находятся на хранении в архивах, географически удаленных друг от друга, изучение особенностей развития какого-либо феномена в области права посредством работы во всех архивах, в которых хранятся нужные правовые акты, является трудной задачей, с учетом, помимо прочего, специфики архивного дела. Именно поэтому необходимо создание информационных порталов, посвященных определенному феномену из сферы права, которые могли бы объединить документы из нескольких архивов, что позволит углубить понимание исторических процессов, тенденции развития юриспруденции и ее отдельных элементов. Опыт создания и наполнения контентом сайта, посвященного заводчикам Демидовым является подтверждением того, что применение цифровых технологий, в том числе и в области изучения истории права, содействует совершенствованию инструментов и средств, позволяющих детально и систематизировано исследовать специфику эволюции разных правовых феноменов.

Список литературы

1. Государственный архив Свердловской области (ГАСО). Ф. 102 «Демидовы, заводовладельцы». 1702–1915 гг. Оп. 1. Д. 95–354.

2. Национальные архивы Франции. Ф. 400AP/84: Канино – Франц II, император Австрии, раздел: Демидов, муж принцессы Матильды. Письма. Документы. Л. 1–256.

3. Неклюдов Е. Г. Уральские горнозаводчики XVIII – начала XX в.: значительные роды // Ученые записки НТГСПИ. Серия: История и филология. 2021. № 4. С. 99–120.

4. Шамнэ Е. Д. Меценатство в России: история и современность // Научно-образовательный потенциал молодежи в решении актуальных проблем XXI века. 2018. № 10. С. 480–483.

5. Antonov M. History of Russian law and its interpretations // Review of Central and East European Law. 2020. Т. 45. № 1. Pp. 161–180.

6. Nikolaev N. Y., Garbuzov D. V., Ramazanov S. P., Yurchenko D. S. Russia and international humanitarian law: history, modernity and prospects // Lecture Notes in Networks and Systems. 2020. Т. 111. Pp. 419–426.

Ю. Е. Воверко,

студент,

Алтайский филиал Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации

А. С. Шаповал,

студент,

Алтайский филиал Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации

ПРЕПЯТСТВИЯ ПРИ ПОДПИСАНИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСЬЮ ДОКУМЕНТОВ ПРИ ЗАКЛЮЧЕНИИ МЕЖДУНАРОДНЫХ СДЕЛОК

Аннотация. В статье отмечены наиболее актуальные вопросы, связанные с препятствиями, возникающими при подписании электронной цифровой подписью документов при заключении международных сделок. Авторами статьи выявлены наиболее острые проблемы при подписании электронных документов компаний из разных стран. Рассматриваются способы решения, которые можно применить на данный момент, с анализом их преимуществ и недостатков. Предложены направления совершенствования регулирования законодательства в этой сфере.

Ключевые слова: право, международное частное право, цифровые технологии, международные сделки, электронная цифровая подпись, электронный документооборот

OBSTACLES ARISING WHEN SIGNING DOCUMENTS BY ELECTRONIC DIGITAL SIGNATURE WHEN CONCLUDING INTERNATIONAL TRANSACTIONS

Abstract. The article highlights the most pressing issues related to the obstacles that arise when signing documents with an electronic digital signature when concluding international transactions. The authors of the article identified the most acute problems

in signing electronic documents of companies from different countries. Solutions that can be applied at the moment are considered, with an analysis of their advantages and disadvantages. In addition, directions for improving the regulation of legislation in this area are also proposed.

Keywords: Law, Private international law, Digital technologies, International transactions, Electronic digital signature, Electronic document management

Пандемия коронавируса 2020 г. оказала влияние на взаимодействие различных субъектов. Закрытие границ, изоляция и различного рода ограничения стали испытанием для этого взаимодействия. В связи с усилением противоэпидемических мер ускорился переход от бумажного документооборота к электронному. Меньше контактов – меньше рисков. Но этот процесс происходит не так быстро, как этого требует ситуация, и тому есть причины. Именно поэтому необходимо усовершенствовать данные процессы.

Электронный документооборот (далее – ЭДО) – это система процессов по обмену документов в электронном виде. Для того чтобы документ имел юридическую силу, необходимо, чтобы его подписали обе стороны. Для использования систем ЭДО необходимо подписание электронной цифровой подписью [5. С. 48–50].

Электронная цифровая подпись (далее – ЭЦП) – это, по сути, аналог обычной подписи, т. е. реквизит, который проставляется на документе, но в электронном формате на основе процедуры криптования. Данный вид аутентификации личности невозможно увидеть, о его наличии свидетельствует кодировка, состоящая из цифр в конце документа [2. С. 67–70].

ЭЦП применяется для упрощения рабочего процесса и ведения документооборота не только организации, но и физических лиц. Благодаря внедрению такой подписи документ в электронном виде становится равноценным бумажному, подписанному от руки.

Существует три вида электронно-цифровой подписи, каждый из которых наделен определенной характеристикой и используется в различных ситуациях.

Простая электронная подпись (ПЭП) – это наименее безопасный вариант подписи, так как она не наделяет электронный файл юридической ролью, пока между сторонами-составителями не будут заключены дополнительные соглашения, касающиеся правил подписания и признания ЭЦП [7. С. 164–173]. Другими словами, контрагент может получить информацию только о ее реквизитах, дате подписания и составителе данного документа.

Для обеспечения большей надежности защиты информации применяется усиленная ЭЦП, которая подразделяется на неквалифицированную и квалифицированную.

Усиленная неквалифицированная ЭЦП представляет собой криптографический шифр, который использует открытый и закрытый ключ. Благодаря этому в документе можно увидеть все правки, так как подпись идентифицирует владельца и контролирует вносимые в документ изменения, после его подписания [6. С. 253–256].

Усиленная квалифицированная подпись имеет ряд существенных отличий, таких как более сложная процедура создания, так как для ее создания нужны определенные криптографические инструменты, подтвержденные компетентными

государственными органами, в России эти функции возложены на Федеральную службу безопасности РФ [3. С. 97–103].

Кроме того, для получения усиленной квалифицированной ЭЦП нужен сертификат электронно-криптографического ключа. Сертификат выдается только удостоверяющим центром, прошедшим аккредитацию в Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации. КЭП имеет полную юридическую силу без дополнительных соглашений и используется на большом количестве платформ [4. С. 89–97].

Но данный вид ЭЦП усложняет свободный обмен электронными документами между странами, потому что необходимо заполнить и передать другой стороне большое количество необходимых документов, например, для идентификации груза. Это служебные, бухгалтерские, перевозочные и иные документы.

Еще одна сложность заключается в том, что каждое государство использует свою уникальную криптографию при ведении электронного документооборота, не совместимую с криптографией других стран. Ситуация ухудшается, когда во взаимодействии участвуют три и более страны.

Когда одна компания одной страны (например, Республики Казахстан) хочет направить другой компании из России документы в электронном виде, подписанные ЭЦП Казахстана, то сталкивается с тем, что документ не может быть проверен средствами ЭЦП России. И с другими странами, например, Республикой Беларусь ситуация аналогична.

Поэтому возникает вопрос: как можно урегулировать данный вопрос для удобства обмена электронными документами, где используются разные способы криптографической проверки? Рассмотрим два способа решения данного вопроса:

1. Вывоз-ввоз криптографии – получение удостоверяющей подписи.

Компания-нерезидент получает НЭП (неквалифицированную электронную подпись) в удостоверяющем центре нужной страны. Для этого нужно лично посетить центр или отправить оригиналы документов, заверенные международным нотариатом.

Но у способа имеются недостатки. Экспорт и импорт криптографии – технологически сложная и дорогостоящая процедура. Вряд ли это может быть применено в качестве основного способа. Кроме того, также необходимо периодическое обслуживание инструментов криптографии удостоверяющими центрами. Но самое главное – электронный документ с НЭП не имеет юридической силы в стране нерезидента. Рассмотрим способ номер два.

2. Участие доверенной третьей стороны (ДТС) – без ввоза-вывоза криптографии.

ДТС – это организация, которая может проверять ЭЦП в электронных документах. Деятельность организации регламентирована фиксированным моментом в отношении лица, подписавшего электронный документ.

При обмене электронными документами между представителями двух стран (G2G) функции ДТС выполняет Минкомсвязь России согласно постановлению от 24 июля 2014 г.

Постановление Правительства Российской Федерации от 24 июля 2014 г. № 698 регламентирует: «Министерство связи и массовых коммуникаций РФ выполняет

функции доверенной третьей стороны при обмене электронными документами в случаях, если ее участие в таком обмене предусмотрено международными договорами Российской Федерации» [1].

Приведем несколько примеров. Компания «Рэйл Коммерс» (РФ) использовала институт доверенной третьей стороны Республики Казахстан в лице АО «Национальные информационные технологии». «Рэйл Эксперт» (РФ) и «Documentolog Global Limited» (Казахстан) в 2021 г. запустили в тестовом режиме сервис обмена цифровыми документами между двумя странами.

Но масштабировать это решение в полной мере пока невозможно. Особенно в тех случаях, когда речь идет о взаимоотношениях между бизнесом и государством или бизнесом и бизнесом (B 2G и B 2B соответственно).

Регламентирующие обмен документы: Положение о ДТС, регламент работы Оператора ДТС, еще не приняты на уровне Правительства России. Что и затрудняет прозрачную организацию трансграничного ЭДО через сервисы ДТС.

Помимо этого, также можно возложить организацию ЭДО на компанию-экспедитора, которая будет присутствовать на территории иностранного государства.

Благодаря статусу резидента и ИНН (идентификационному номеру налогоплательщика) можно получить ЭЦП, которая действует в данной юрисдикции, и впоследствии использовать ее при оформлении документов со всеми участниками.

Данный способ взаимоотношений ЭДО дает определенные преимущества клиентам компании-экспедитора. Ведь компания берет на себя риски и возникающие в работе с ЭДО при международных перевозках, а клиент получает подтверждающие документы, соответствующие требованиям государства, на территории которого он находится.

Однако, способ подходит только клиентам компании экспедитора, и не решает проблемы правового регулирования и проблему перевыставления документов внутри группы компаний. Для развития международного ЭДО необходимо государственное сотрудничество по вопросам упрощения процедуры.

В качестве решения можно предложить следующие действия:

1. Разработка открытого международного договора о признании ЭЦП на территории государств-участников договора. Примерный алгоритм действий следующий: сначала подписывается международный договор, затем нужно придумать класс ЭЦП с международной квалификацией (с пометкой о возможности применения в международных сделках в рамках подписанной конвенции с участием стран. Заявление пишется в российский уполномоченный орган на двух языках (русский и той страны, с кем планируется сотрудничество), далее заявление получает уполномоченный орган другой страны, верифицируется и наш орган выдает подпись.

2. Внесение изменений в ФЗ «Об электронной подписи» от 06.04.2011 № 63-ФЗ. Определить в законе компетентный орган, который будет выдавать документ и проводить необходимую процедуру.

3. Приведение законодательства об ЭЦП в соответствии с предложенными изменениями.

Данное предложение облегчит сотрудничество международных компаний, поспособствует развитию электронного документооборота.

Список литературы

1. Винтайкина Д. А. Сферы и преимущества использования электронной цифровой подписи / Д. А. Винтайкина, Ю. Р. Астанаева // Научно-исследовательский центр «Technical Innovations». 2021. № 3. С. 67–70.
2. Гончаров Е. И. Проблемы применения цифровой подписи в электронном документообороте России / Е. И. Гончаров, Т. В. Шатковская // Северо-Кавказский юридический вестник. 2020. № 2. С. 97–103.
3. Квашнин В. И. Об условиях ведения международной электронной коммерции в России с использованием электронной цифровой подписи // Вестник Санкт-Петербургского университета. Право. 2009. № 3. С. 89–97.
4. Ковалева О. В. Электронная цифровая подпись: преимущества и недостатки // Информационные войны. 2020. № 2 (54). С. 48–50.
5. Курочкина Е. А. Возможности использования электронно-цифровой подписи в современных условиях / Е. А. Курочкина, Т. М. Тарасова // Наука и образование транспорту. 2020. № 1. С. 253–256.
6. О внесении изменения в Положение о Министерстве связи и массовых коммуникаций Российской Федерации: Постановление Правительства РФ от 24.07.2014 № 698. URL: <http://www.pravo.gov.ru> (дата обращения: 22.07.2022).
7. Подоляк А. А. Система электронного документооборота и международный опыт ее применения // Трибуна ученого. 2020. № 6. С. 164–173.

Г. Е. Волкова,

соискатель кафедры теории и истории государства и права,
Южный федеральный университет

ТРАНСФОРМАЦИЯ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

Аннотация. Усиливающееся влияние цифровых технологий на систему государственного управления, формирование соответствующей правовой системы, появление нового цифрового или информационного пространства делают актуальными научные исследования в сфере проблематики охраны и защиты прав человека и гражданина. В статье рассматривается влияние цифровых технологий на обеспечение и защиту конституционного права на неприкосновенность частной жизни, которое подвергается постепенной трансформации, рискуя раствориться в цифровом пространстве.

Ключевые слова: цифровые технологии, цифровизация правоотношений, права человека, неприкосновенность частной жизни, цифровое государство, цифровой портрет

TRANSFORMATION OF THE RIGHT TO PRIVACY IN THE CONDITIONS OF DIGITALIZATION OF SOCIETY

Abstract. The increasing influence of digital technologies on the public administration system every year, the formation of an appropriate legal system, the emergence of a new digital or information space make scientific research in the field of

protection and protection of human and civil rights relevant. The article examines the impact of digital technologies on the provision and protection of the constitutional right to privacy, which is undergoing a gradual transformation, risking being dissolved in the digital space.

Keywords: Digital technologies, Digitalization of legal relations, Human rights, privacy, Digital state, Digital portrait

Развитие информационно-коммуникационных в совокупности с принятым государством курсом на цифровизацию оказывает значительное влияние на давно устоявшиеся правовые институты, что приводит к необходимости либо переосмысления существующей системы представлений об основных конституционных правах личности, либо формированию системы нового поколения прав, именуемых «цифровыми правами».

Происходящая цифровая трансформация создает как новые возможности, так и риски для благополучия человека, что обуславливает объективную потребность изменений существующего законодательства. Особенно уязвимым в цифровую эпоху становится право на неприкосновенность частной жизни, т.к. наличие информационных технологий, например таких, как Big Data, позволяющей обрабатывать ежесекундно колоссальное количество данных, нарушает это право в силу своей природы.

Тотальный автоматизированный контроль за сферой частной жизни лица «становится технической нормой экономической жизни через внедряемые цифровые сервисы и технологии, требующие обработки персональных данных без согласия лица, как то идентификации личности: геоданные, сетевая активность, мониторинг речи пользователя и т.д.» [5. С. 11]. Существующий при этом риск утечки личной информации и персональных данных, несовершенство систем информационной безопасности, рост числа правонарушений в цифровом пространстве, а также сбор излишней информации о субъекте права в коммерческих целях позволяют рассуждать о возможности перехода любых сведений, составляющих приватность, в публичное достояние.

В существующих реалиях неизбежно возникают вполне резонные вопросы: насколько распространение и использование цифровых технологий во всех сферах жизнедеятельности человека обеспечивает соблюдение конституционного права каждого на неприкосновенность частной жизни? Возможно ли вообще сохранить право на неприкосновенность частной жизни в условиях цифровой реальности?

Право на неприкосновенность частной жизни – это одно из основополагающих конституционных прав человека, провозглашенное ст. 23 Конституции РФ. Право на неприкосновенность частной жизни отличает от других личных немущественных прав возможность определения границ его охраны самостоятельно их носителем. Осуществление самостоятельного контроля за распространением информации о себе и своей частной жизни — неотъемлемый элемент реализации права на неприкосновенность частной жизни, что неоднократно подчеркивал в своих определениях Конституционный Суд Российской Федерации. Возможно ли осуществление такого контроля в цифровой среде? Думается, что нет.

Категория «частная жизнь» в современном российском законодательстве не имеет четких юридических границ, что обусловлено сложностью, многоаспектностью и многогранностью этого понятия. Информация, которую можно отнести к частной, охватывает различные сферы индивидуальной жизнедеятельности человека, границы которых каждый человек определяет по-своему исходя из личных убеждений. Полагаем возможным остановиться лишь на некоторых из них, наиболее уязвимых в цифровую эпоху.

Одним из составляющих права на неприкосновенность частной жизни, подвергающейся трансформации, является право «быть в одиночестве» или право на уединение, которое предоставляет субъекту права возможность совершать или не совершать действия, исходя из уверенности в том, что за ним никто не наблюдает и не подслушивает. В условиях развития технологий биометрической идентификации личности с помощью систем искусственного интеллекта, предоставляющей возможность постоянного наблюдения за каждым человеком, без сформированной на основе широких общественных обсуждений и в отсутствие конкретной нормативной правовой базы данное право рискует «уйти в прошлое».

Особый интерес в свете развития информационных технологий представляет трансформация «права на анонимность» и «права на конфиденциальность», представляющих собой право субъекта самостоятельно определять порядок раскрытия своей личности при реализации данных свобод, предъявлять требования сохранения тайны личности к лицам, которым данные сведения стали известны, а также требование воздержаться от сбора такой информации [2. С. 34].

Цифровые следы («интернет следы», «интернет отпечатки», «digital footprint»), которые мы ежедневно оставляем в информационном пространстве после анализа и обобщения, проведенного с помощью возможностей искусственного интеллекта, могут сформировать наш цифровой портрет, содержащий более точные сведения о нас, вплоть до оценки психоэмоционального состояния, чем те, которые можно было бы узнать из личного общения или психологических тестов. «Вся информация о человеке становится доступной отдельным организациям и лицам, т. е. фактически речь идет о нарастающей угрозе утраты индивидуальной свободы и автономии личности» [5. С. 86]. В качестве примера возможностей вторжения технологий «Больших данных» в личную сферу можно назвать случай, когда американская сеть супермаркетов Target путем автоматизированного статистического анализа покупок узнала о беременности покупательницы и направила ей персонализированную рекламную листовку, содержащую скидочные купоны на подгузники и детское питание, раньше чем члены ее семьи.

Отдельно стоит остановиться на возможности обеспечения конфиденциальности «метаданных», т.е. данных о данных, относящихся к дополнительной информации о содержимом или объекте. Так, загружая фотографию для социальных сетей, мы передаем значительный объем информации, относящейся к изображению. В частности, дату создания изображения, сведения об устройстве, с помощью которого сделано изображение (модель и серийный номер камеры, параметры фокусного расстояния и режима вспышки), в том числе и географические

координаты места, в котором сделана фотография [7]. По сути, «метаданные» могут содержать больше информации, которую можно отнести к личной, чем само изображение.

Обеспокоенность с точки зрения гарантированности конституционного права на неприкосновенность частной жизни в цифровую эпоху вызывает и не имеющее жесткой правовой регламентации право на конфиденциальность пользователей Интернета вещей. Интернет вещей позволяет осуществлять поиск людей, их идентификацию, контролировать действия и передвижения объектов контроля, давать их точную психологическую характеристику и многое другое. Стремительно растущая популярность технологий «умного дома» позволяет передавать в Сеть огромные потоки информации личного характера. Одним из направлений цифровой трансформации системы образования является использование технологий «Искусственного интеллекта» для оказания медицинских услуг, что влечет за собой возникновение новых рисков обеспечения информационной безопасности в этой сфере. Использование «умных устройств» медицинского сегмента, которые предназначены для мониторинга, контроля и поддержания состояния здоровья (аппараты искусственного дыхания, кардиографы, кардиостимуляторы и т.д., а также фитнес-браслетов ставит под угрозу возможность сохранения врачебной тайны как одного из элементов частной жизни. Ожидается, что медицинские устройства и приложения будут иметь дело с жизненно важной частной информацией, такой как персональные медицинские данные, включая генетическую информацию [1].

Полагаем, что в новой цифровой среде люди должны иметь право и возможность осуществлять действенный и эффективный контроль за доступом и распространением личной информации, должны быть разработаны и приняты правовые акты, цель которых заключается в предоставлении физическим лицам эффективных и оперативных средств информирования их о том, что происходит с их персональными данными. Однако сегодня российское законодательное регулирование значительно отстает от фактического развития цифровых общественных отношений, что, безусловно, формирует проблемы нарушения гражданских прав [5. С. 13].

Так можно ли говорить о частной жизни в условиях, когда правовое регулирование возникающих новых «цифровых» отношений отстает от достижений научного технического прогресса, а каждое наше действие в сети Интернет оставляет «цифровой след», а сфера Big date фиксирует и «запоминает» каждое наше цифровое действие? Полагаем, при таких условиях право на неприкосновенность частной жизни имеет все шансы стать декларативным, превратиться в атавизм конституционного права и полностью раствориться в цифровой среде.

Развитие системы электронного контроля, разрабатываемого с помощью цифровых технологий и Big Date, в ближайшее время в корне изменит представление о государстве и праве [4. С. 104]. И нельзя не согласиться с мнением А. И. Овчинникова, что «сегодня перед правоведами стоит задача защитить человечество от поглощения технократической парадигмой цифровой цивилизации» [3. С. 93]. Использование возможностей искусственного интеллекта, создание

банков кредитных историй, сбор информации о каждом гражданине, вплоть до таких банков данных как национальные базы данных ДНК; системы видеоконтроля с идентификацией, — все это дает возможность обеспечения государством безопасности личности от различных угроз, в том числе и террористических, однако может и привести к «созданию тотального электронно-банковского концлагеря» [5, с. 180] и исчезновению самого явления неприкосновенности частной жизни. Можно уже говорить об иллюзии неприкосновенности частной жизни в цифровой среде, об угрозе трансформации в атавизм конституционного права. Для недопущения этого, считаем, что принцип неприкосновенности частной жизни в условиях цифрового общества и государства должен стать основополагающим с точки зрения воспрепятствования цифровым формам тоталитаризма.

Список литературы

1. Аксенова Е. И., Горбатов С. Ю. Применение технологий интернета вещей в здравоохранении // Здоровье мегаполиса. 2021. № 4. URL: <https://cyberleninka.ru/article/n/primeneniye-tehnologiy-interneta-veschey-v-zdravoohranenii> (дата обращения: 24.08.2022).

2. Кузнецова С. С. Право на анонимность в сети Интернет: актуальные вопросы реализации и защиты // Российское право: образование, практика, наука. 2020. № 5. С. 33–41.

3. Овчинников А. И. Права человека в условиях цифровой трансформации общества и государства // Вестник юридического факультета Южного федерального университета. 2021. Т. 8. № 4. С. 93–98.

4. Овчинников А. И., Фатхи В. И. Цифровые права как объекты гражданских прав // Философия права. 2019. № 3 (90). С. 104–112.

5. Правовая политика Российского государства в условиях цифровой экономики и цифрового технологического уклада / А. И. Овчинников, А. Ю. Мамычев, А. Г. Кравченко [и др.]. Москва : Общество с ограниченной ответственностью «Перспектив», 2021. 184 с.

6. Северухин В. А. Проблемы защиты права на неприкосновенность личной жизни в контексте цифровизации // Вестник МГПУ. Серия: Юридические науки. 2020. № 2(38). С. 85–98.

7. Эксперимент: проверяем, что интересного можно узнать из метаданных фотографий в Интернете: блог Касперского. URL: <https://www.kaspersky.ru/blog/exif-privacy/13506/> (дата обращения 05.09.2022).

А. А. Габович,
старший преподаватель,
кафедра конституционного и муниципального права,
Ростовский государственный экономический университет

ФОРМИРОВАНИЕ ГРАЖДАНСКОЙ ПОЗИЦИИ СТУДЕНТОВ – БУДУЩИХ ЮРИСТОВ В КОНТЕКСТЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. В статье анализируется опыт Юридической клиники Ростовского государственного экономического университета по оказанию бесплатной юридической помощи нуждающимся категориям граждан, влияние клинического образования на формирование гражданской позиции будущих юристов и их профессиональное становление. Анализируются основные мероприятия, способствующие получению профессиональных компетенций будущих юристов, рассматривается воздействие образовательной среды университета на формирование гражданской позиции студентов – будущих юристов в контексте цифровой трансформации.

Ключевые слова: юридическая клиника, бесплатная юридическая помощь, негосударственная система бесплатной юридической помощи, гражданская позиция будущих юристов, клиническое образование, практическая подготовка, юрист

FORMATION OF CIVIC POSITION STUDENTS – FUTURE LAWYERS IN THE CONTEXT OF DIGITAL TRANSFORMATION

Abstract. The article analyzes the experience of the Legal Clinic of the Russian State Economic University (RINH) in providing free legal assistance to needy categories of citizens, the impact of clinical education on the formation of the civil position of future lawyers and their professional development. The main activities contributing to the acquisition of professional competencies of future lawyers are analyzed, the impact of the educational environment of the university on the formation of the civil position of students – future lawyers in the context of digital transformation is considered.

Keywords: Legal clinic, Free legal aid, Non-governmental system of free legal aid, Citizenship of future lawyers, Clinical education, Practical training, Lawyer

Юридическая клиника РГЭУ (РИНХ) является участником негосударственной системы бесплатной юридической помощи, осуществляет свою деятельность в соответствии с положением о Юридической клинике РГЭУ (РИНХ).

Целью Юридической клиники РГЭУ (РИНХ) является создание условий для реализации установленного Конституцией Российской Федерации права граждан на получение квалифицированной юридической помощи и защиты их законных интересов.

Для реализации данных целей в РГЭУ (РИНХ) создано отдельное структурное подразделение – Юридическая клиника РГЭУ (РИНХ), осуществляющая свою деятельность на постоянной основе и являющаяся базой для практической подготовки студентов университета.

Юридическая клиника РГЭУ (РИНХ) оказывает бесплатную юридическую помощь нуждающимся гражданам и сотрудникам РГЭУ (РИНХ).

Юридическая помощь предоставляется бесплатно. Распространенными формами предоставления помощи являются: устное консультирование, составление обращений в организации и государственные органы, проектов исковых заявлений в суды.

Анализ поступивших обращений в Юридическую клинику РГЭУ (РИНХ) за 2021 г. свидетельствует, что граждане больше всего обращаются за помощью по гражданским и финансовым делам. Большинство обращений поступает от пенсионеров, которым необходима юридическая помощь. Среди наиболее частых обращений: банкротство по кредитным обязательствам, споры по начислению пенсий, конфликты между соседями, обжалование судебных решений и несогласие с действиями должностных лиц.

При поступлении обращения в Юридическую клинику РГЭУ (РИНХ) секретарем производится его регистрация с фиксацией контактных данных гражданина и сути его обращения, далее определяется преподаватель-куратор и студенты, которые будут оказывать юридическую помощь гражданину.

Информационную поддержку в освещении деятельности Юридической клиники РГЭУ (РИНХ) оказывает медиацентр РГЭУ (РИНХ), СМИ, а также органы государственной власти Ростовской области, на страницах которых размещена информация о возможности обратиться за получением бесплатной юридической помощи.

Новое направление в работе Юридической клиники РГЭУ (РИНХ) – оказание бесплатной юридической помощи жителям Донецкой и Луганской народных республик. За несколько месяцев была оказана помощь 32 беженцам по процедуре вступления в гражданство Российской Федерации, принятия наследства, получения социальных выплат от государства. Преподаватели-кураторы и студенты в каждом конкретном случае используют индивидуальный подход к гражданам, обратившимся за помощью в Юридическую клинику РГЭУ (РИНХ).

Новой формой предоставления юридической помощи гражданам стало консультирование в дистанционном режиме с использованием аудиосвязи и видеосвязи. Как показала практика, данная форма имеет существенное преимущество: возможность оказывать юридическую помощь вне зависимости от места нахождения гражданина, буквально из дома, что важно для обеспечения конституционных гарантий прав граждан старшего поколения и с ограниченными возможностями на получение юридической помощи.

Однако выявлены и недостатки, такие как: невозможность подтвердить личность гражданина, обратившегося за помощью, ознакомиться с документами, необходимыми для осуществления юридической консультации, а в отдельных случаях, при низком качестве связи, периодически происходят сбои во время оказания юридической консультации.

Представляется возможным урегулирование данных проблемных вопросов на законодательном уровне.

Юридическая клиника РГЭУ (РИНХ) создает условия для развития практических компетенций выпускников, получения первичных навыков взаимодействия с гражданами, что способствует формированию их гражданской позиции. С 2016 по 2021 г. в Юридической клинике РГЭУ (РИНХ) 458 студентов прошли практику

и оказали 1089 консультаций. При прохождении практики за студентами закрепляются преподаватели-кураторы из числа сотрудников юридического факультета РГЭУ (РИНХ), которые осуществляют координацию прохождения практики студентами.

Положительным является опыт рассмотрения обращений совместно с депутатами и членами общественных палат, что способствует всестороннему рассмотрению обращений граждан, а также получению первичных профессиональных компетенций обучающихся. Как показала практика, при рассмотрении обращений граждан, связанных с нарушениями их прав, весьма эффективным является их сопровождение со стороны депутатского корпуса, что обусловлено возможностью направления депутатского запроса или личного контроля со стороны члена Общественной палаты.

Так, в марте 2022 г. Юридическая клиника РГЭУ (РИНХ) традиционно присоединилась к проведению Единого дня оказания бесплатной юридической помощи, в котором принял участие депутат Государственной Думы Федерального Собрания РФ Л. Н. Тутова и декан юридического факультета РГЭУ (РИНХ), председатель комиссии по развитию институтов гражданского общества, общественному контролю и защите прав человека Общественной палаты Ростовской области А. Н. Позднышов. В ходе оказания юридической помощи удалось помочь пенсионеру с инвалидностью разъяснить процедуру обжалования судебных решений, подготовить проект обращения в Прокуратуру Ростовской области и дать подробные консультации по вопросам от жителей Донецкой и Луганской народных республик.

В целом можно констатировать, что Юридическая клиника РГЭУ (РИНХ) гарантирует реализацию конституционных прав граждан на получение квалифицированной юридической помощи и формирование у будущих юристов активной гражданской позиции.

С. Р. Гадельшина,

студент,

Томский государственный университет систем
управления и радиоэлектроники

Д. С. Вебер,

студент,

Томский государственный университет систем
управления и радиоэлектроники

ЧАТ-БОТЫ КАК ИНСТРУМЕНТАРИЙ СОВРЕМЕННОГО ЮРИСТА

Аннотация. В статье рассматриваются особенности использования чат-ботов в деятельности юриста и компаний. Также проводится анализ известных чат-ботов, работающих по юридическому направлению, на платформе Telegram, сравниваются достоинства и недостатки при применении чат-ботов, в качестве помощника юриста. В процессе исследования были применены общенаучные (диалектический и дедуктивный методы), анализ и частнонаучные (метод сравнения) методы.

Ключевые слова: чат-бот, искусственный интеллект, право, цифровые технологии, современные технологии, юридическая деятельность

CHATBOTS AS A TOOLKIT FOR THE MODERN LAWYER

Abstract. The article discusses the use of chatbots in the activities of lawyers and companies. It also analyzes the well-known chatbots, working in the legal field, on the Telegram platform, compares the advantages and disadvantages of using chatbots as a paralegal. General scientific (dialectical and deductive methods), analysis and special scientific (method of comparison) methods were used in the research.

Keywords: Chatbot, Artificial intelligence, Law, Digital technologies, Modern technologies, Legal activity

Введение. В 1966 г. программа ELIZA Джозефа Вейценбаума смогла обмануть пользователей, заставив их поверить, что они ведут текстовый разговор с реальными людьми. Это первое применение машин, имитирующих настоящую вещь, было только началом, поскольку ключевой метод работы Вейценбаума будет скопирован и использован даже по сей день [2]. За последние пять лет функциональность чат-ботов вышла далеко за рамки того, что было вначале. НЛП и ИИ в чат-ботах добились огромного прогресса, и теперь чат-ботов можно найти в любой отрасли: учебных заведениях или частных школах, региональных авиакомпаниях, международных логистических компаний, коммунальных энергетических компаний и т. д.

Основная часть. Чат-бот (от англ. – chatbot) – это тип цифрового помощника, который имитирует человеческий разговор с пользователем посредством различных технологий коммуникации, синтезируя голос или предлагая кнопки принятия решения.

Чат-боты существуют абсолютно в разных социальных сетях, чем упрощает создание и пользование для юриста. Ему остается лишь выбрать удобную платформу для своей работы и заказать, либо же создать, чат-бота.

Одним из таких сервисов является WhatsApp, насчитывающий более 1,3 млрд пользователей. Также WhatsApp выпустил приложение, специально предназначенное для компаний, чтобы более эффективно общаться со своими пользователями на сайте. Кроме того, этот набор инструментов включает в себя возможность создания чат-ботов. Исследование Morning Consult говорит о том, что более 80 % компаний малого бизнеса в Индии и Бразилии сказали, что сегодня WhatsApp помогает им общаться с клиентами, а их бизнесу расти [4].

Еще одной популярной сетью является Telegram. В нем можно заводить собственные каналы, создавать чаты-комьюнити, чат-ботов и т. д. В 2021 г. приложение Telegram попало в топ-5 самых популярных в мире. Согласно исследованию Sensor Tower, в первом квартале 2021 г. мессенджер установили более 100 млн пользователей. Среди мессенджеров больше установок только у WhatsApp – 125 млн [1].

Для наглядного рассмотрения работы юридических чат-ботов можно взять последний мессенджер – Telegram.

@LawyerDocs_bot – это бот для бесплатного составления юридических документов. Предоставляет консультации с юристами и адвокатами. После нажатия кнопки «/start» бот выдает следующую информацию: «Добро пожаловать! Я бот, который поможет подготовить для вас бумаги на одно из выбранных направлений!

Также я могу помочь обратиться в суд и собрать необходимые документы. Просто следуйте моим инструкциям. Давайте приступим! После нажатия одной из кнопок, вы автоматически подтверждаете согласие на обработку ваших персональных данных. Теперь вы можете выбрать, какая помощь для подачи документов, вам требуется». В пункте управления ботов пользователю будут доступны несколько разделов, но для анализа бота необходимо выбрать «составление документов». В конечном итоге посетитель может либо самостоятельно заполнить заявление с помощью чат-бота, либо связаться с профессиональным юристом для решения своего вопроса.

В целях примера использования чат-бота авторы попробовали создать юридический документ. В конечном итоге для полного заполнения документа потребовалась всего пара минут, впоследствии клиент получает конечный вариант заявления, которое необходимо распечатать и подписать.

В свою очередь, у LawyerDocs_bot есть перечень опций, бот может сформировать таких документы, как:

- Ходатайство на УДО.
- Обжалование штрафа по видеофиксации.
- Составление апелляционной жалобы на постановление мирового судьи по делу об административном правонарушении.
- Составление заявления в суд на развод.
- Обжалование действий и бездействий управляющих компаний в сфере ЖКХ.
- Обжалование судебного приказа.
- Составление жалоб по защите прав потребителя.

Если оценивать со стороны грамотности, то вышеозначенный бот нуждается в незначительных модификациях в сфере итогового варианта документа. Но, несмотря на это, чат-бот доведен до идеального варианта использования, абсолютно любой пользователь сможет получить юридический документ, лишь ответив на перечень вопросов.

Еще одним рассматриваемым ботом на платформе Telegram станет @LawProInfoBot «Помощник юриста» – один из самых полезных инструментов для юристов на данной платформе. Данный бот автоматически проверяет сайт ГАС «Правосудие» на изменение по делам и присылает уведомления в случае изменений. В способности этого чат-бота входят:

- Выписка из ЕГРЮЛ/ЕГРИП.
- Информация о судебных делах (СОЮ, МосГорСуд, мировые суды).
- Информация о наличии долгов и возбужденном исполнительном производстве.
- Автоматическое уведомление об изменениях в карточке судебного дела (подписка на дела).

Этот бот направлен на адвокатов, юристов, адвокатские компании, работников аппарата суда и многих др.

Благодаря боту профессиональные юристы смогут избавиться от мониторинга информации на сайтах судов (в ручном режиме), отследить статус дел в едином окне, запросить выписку из ЕГРЮЛ, получать информацию об исполнительном производстве и т. д.

Несмотря на то, что чат-бот был запущен более года назад, его улучшают по сей день, например, добавление возможности делать заметки в списке «отобранных дел», просмотр списка назначенных к рассмотрению дел на указанную дату, добавлять заседание в календарь с возможностью напоминания о судебных заседаниях. Он является единственным ботом, работающим с судами общей юрисдикции.

После наглядных примеров использования чат-ботов следует выделить прехвосходства и недостатки.

В качестве положительных сторон можно выделить следующее:

– Доступность. Чат-боты могут мгновенно отвечать клиентам в любое время суток, и разница в часовых поясах никакой сложности играть не будет. Примером может служить компания Cartland Law, которая внедрила к себе бота для составления типовых документов и поиска информации. После чего эффективность компании в разы возросла [5].

– Уменьшение количества ошибок. Чат-боты помогают свести к минимум ошибки. Люди могут ошибаться при предоставлении информации клиентам, но поток чат-бота содержит заранее написанную информацию, интеллектуальные алгоритмы и программирование, что обеспечивает правильный вывод данных.

– Многоплатформенность. Чат-боты предлагают многоканальное обслуживание клиентов и могут одновременно работать в нескольких сервисах.

– Создание юридических документов. Вручную это требует много времени для юристов. Юридические чат-боты высвобождают время юриста, автоматизируя и создавая контракты, соглашения о неразглашении и другие типы юридических документов с помощью определения ключевых слов. Согласно зарубежному исследованию Clío, только 29 % времени юристов в среднем оплачивают клиенты. Остальное уходит на административные, финансовые, маркетинговые задачи, часть из которых можно доверить чат-ботам [3].

В качестве отрицательных сторон можно выделить:

– Пользователи, использующие приложениями WhatsApp/Viber для массовых рассылок от чат-ботов, должны осознавать риск, что они могут быть заблокированы из-за излишней активности, из чего последует утрата номера.

– Ответы на нетипичные вопросы. Так как чат-боты создаются реальными людьми, невозможно угадать количество вариаций тех или иных вопросов, формулировок и т. д., что может поставить чат-бота в ступор.

– Оптимизация чат-ботов. Необходимо обновлять своего бота для поддержки актуальной информации.

Вывод. Чат-боты более эффективны в общении с большой аудиторией, чем люди. Они могут становиться полезным инструментом сбора информации в ближайшем будущем. Юридические чат-боты предлагают мгновенную поддержку не только юристам, но и обычным пользователям по всем каналам. Чат-боты позволяют юристам упростить доступ к юридическим исходным материалам с любого устройства и в любой момент дня.

Список литературы

1. Аудитория Телеграма в 2022 году: насколько выросла и как это использовать бизнесу. URL: <https://smmplanner.com/blog/auditoriia-tielieghrama-v-2022-ghodunaskolko-vyroslo-i-kak-eto-ispolzovat-bizniesu/> (дата обращения: 01.09.2022).
2. Как первый в мире чат-бот приобрел черты искусственного интеллекта, и что из этого вышло. URL: https://www.iguides.ru/main/other/kak_pervyy_v_mire_chat_bot_priobrel_cherty_iskusstvennogo_intellekta_i_chno_iz_etogo_vyshlo/ (дата обращения: 10.09.2022).
3. Как с помощью чат-бота сократить расходы на клиентскую поддержку и сохранить лояльность пользователей? URL: <https://markswebb.ru/report/chatbot-rank-2021/#calculation> (дата обращения: 23.08.2022).
4. Представляем приложение WhatsApp Business. URL: <https://blog.whatsapp.com/introducing-the-whats-app-business-app> (дата обращения: 01.09.2022).
5. Ailira. The way law should be. URL: <https://www.ailira.com/> (дата обращения: 23.12.2021).

Н. А. Галкин,
магистрант,

Московский городской педагогический университет

ВЛИЯНИЕ «ИНТЕРНЕТА ВСЕГО» НА ПРАВО

Аннотация. Тезисы посвящены прогнозу влияния технической революции в области микропроцессоров на право. Данный феномен именуется как «интернет всего». В рамках статьи приводятся примеры использования чипов и то, как это изменит правоприменение. Актуальность исследования заключается в том, что интернет вещей уже изменил не только повседневную жизнь людей, но и правоприменение, поэтому логично будет предположить, что внедрение информационно-коммуникационных сетей в каждую вещь в мире будет новой технологической революцией, которая изменит все отношения, включая правовые.

Ключевые слова: интернет всего, интернет вещей, микропроцессоры, умные гаджеты, Data Matrix, QR-код, правовое регулирование сети Интернет

THE IMPACT OF THE INTERNET OF EVERYTHING ON THE LAW

Abstract. The thesis focuses on predicting the impact of the microprocessor technological revolution on the law. This phenomenon is referred to as the 'Internet of Everything'. Within the framework of the article examples of the use of chips and how it will change law enforcement are given. The relevance of the research lies in the fact that the Internet of things has already changed not only people's daily lives but also law enforcement, so it is logical to assume that the introduction of information and communication networks in everything in the world will be a new technological revolution that will change all relationships, including legal ones.

Keywords: Internet of things, Internet of things, Microprocessors, Smart gadgets, Data Matrix, QR code, Legal regulation of the Internet

Все хоть немного слышали об интернете вещей, т. е. когда бытовые приборы подключаются к сети Интернет и становятся «умными». Сейчас все же говорят о наступлении новой эпохи развития Интернета, так называемом интернете всего, когда каждая вещь будет подключена к информационно-телекоммуникационной сети Интернет. И все это будет возможно благодаря микропроцессорам.

В наше время микропроцессоры можно встретить в смартфонах, планшетах, компьютерах и множестве других технически сложных устройств. Если говорить об истории, то первое такое устройство появилось в 1971 г., и им является Intel 4004 [3], которая могла лишь совершать простые математические действия. Микросхема была сделана по технологии 10000 нанометров, для сравнения, современные микропроцессоры – от 5 до 15 нанометров (рис. 1).

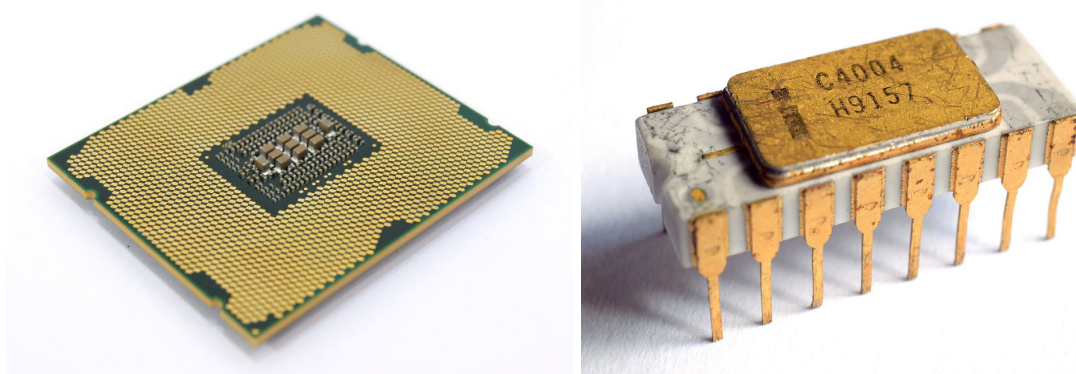


Рис. 1. Визуальное сравнение микропроцессоров Intel 4004 (справа) и Intel Core i7 (слева)

Также следует отметить, что по своей природе микропроцессор является квазиизобретением, так как благодаря ему можно делать другие изобретения. Как это и происходит уже несколько десятков лет. Благодаря этим устройствам любой человек может не просто пользоваться сетью Интернет, а общаться, несмотря на расстояния, заказывать такси, еду, делиться своим творчеством, пользоваться государственными услугами и многое др. Даже за последние десять лет наша жизнь сильно изменилась благодаря технологиям. А что говорить про 50 лет назад. За это время чипы стали меньше, более энергоэффективными и мощными. Здесь стоит привести пример новой технологии. В 2021 г. компания ARM представила пластиковые микропроцессоры Plastic ARM [1]. Они являются тонкими, гибкими, а их стоимость не превышает одного цента. Благодаря данной технологии чип можно внедрить в любую вещь, что не приведет к повышению ее цены.

Возвращаясь к раскрытию понятия «интернета всего», следует привести пример широкого использования чипов. С помощью вышеописанной технологии можно внедрять чипы во все предметы, при этом без повышения цены. Так, например, с помощью умных ценников можно получать полную информацию о товаре или, например, умная упаковка для продуктов сможет посылать уведомления о том, что срок годности молока в вашем холодильнике подходит к концу. Да, многие скажут, что в целом есть похожая инициатива с обязательной маркировкой товаров

и программой «Честный знак» [2]. Но данная технология уступает чипам в своей применимости. Так как используется цифровой код Data Matrix – двумерный штрих-код. Да, он содержит в себе больше информации, чем QR-код, но чипы способны на большее, они могут самостоятельно посылать сигналы, а код можно только сканировать для получения информации.

Также, например, возможна умная одежда: носки с шагомером, футболка, считывающая температуру тела и пульс, штаны, измеряющие артериальное давление. Да, умная одежда уже существует, но данная технология основана на кремниевых чипах, которые утяжеляют одежду, повышают ее цену и не являются износостойкими. Таким образом, применение чипов многогранно.

Полностью разобравшись с данной технологией и понятием «интернет всего», можно сделать некие прогнозы его влияния на право.

Начнем с хорошего: если возвращаться к примеру с умными упаковками продуктов питания, то можно точно сказать, что если система будет самостоятельно посылать работникам супермаркетов уведомления о том, что у таких-то продуктов закончился срок годности, то снизится количество возвратов товаров ненадлежащего качества и в целом количество исков по защите прав потребителей, что значительно разгрузит суды.

Если в каждой вещи будет чип, который можно отследить, то в целом это может снизить количество краж, так как предметы будут легко отследить.

Если думать о плохой и умной одежде, то можно предположить, что злоумышленники могут получить информацию о передвижениях пользователя для своих корыстных целей. С другой стороны, в телефонах уже давно есть GPS, с помощью которого тоже можно отследить передвижения.

Также может возникнуть проблема с персональной информацией и личными данными. Если каждая вещь в доме будет подключена к сети Интернет, может произойти утечка личной информации пользователя, которая может попасть к злоумышленникам.

Безусловно, перечисленное в статье является лишь прогнозом, основанным на технологиях, и никто точно не знает, по какому пути развития пойдут технологии. Единственное, что можно сказать, так то, что право вторично по отношению к технологиям, мы видим это и сейчас. Вначале появляется новая технология, которая меняет обыденную жизнь граждан, и законодатель видит, что эти отношения нужно ввести в правовое поле, и после этого появляется нормативно-правовой акт.

Закончить данное рассуждение хотелось бы цитатой футуролога Жака Фреско: «Люди не понимают потрясающих возможностей разумного использования технологий».

Список литературы

1. Встречаем PlasticARM – 32-битный гнущийся процессор (26 июля 2021 г.) // Новостной портал Хабр. URL: <https://habr.com/ru/company/ruvds/news/t/569636/> (дата обращения: 04.09.2022).
2. Официальный сайт государственной системы маркировки и прослеживания Честный ЗНАК. URL: <https://честныйзнак.рф> (дата обращения: 04.09.2022).
3. Intel 4004 // Материал из Википедии – свободной энциклопедии. URL: https://ru.wikipedia.org/wiki/Intel_4004 (дата обращения 04.09.2022).

Ю. Н. Гамбеева,

старший преподаватель кафедры управления,
Филиал Московского государственного университета
имени М. В. Ломоносова в городе Севастополе

Н. Н. Кожухова,

старший преподаватель кафедры управления,
Филиал Московского государственного университета
имени М. В. Ломоносова в городе Севастополе

РАЗВИТИЕ ИНСТИТУТА САМОЗАНЯТОСТИ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ПЛАТФОРМ

Аннотация. В статье рассматриваются вопросы цифровой трансформации и инфраструктурного развития рынка труда, которые привели к появлению новым форм организации трудовой деятельности – самозанятости и платформенной занятости. В работе определено, что введение специального налогового режима и упрощенного порядка регистрации способствовали тому, что самозанятость стала одним из самых динамично развивающихся институтов в России. Выявлено, что, несмотря на регулирование отношений платформ с самозанятыми гражданами в нормативно-правовом поле имеются определенные трудности, платформенная занятость играет позитивную социально-экономическую роль в обществе.

Ключевые слова: самозанятость, платформенная занятость, специальный налоговый режим, цифровые платформы, цифровые технологии, цифровая трансформация, рынок труда

DEVELOPMENT OF THE INSTITUTION OF SELF-EMPLOYMENT USING DIGITAL PLATFORMS

Abstract. The article deals with the issues of digital transformation and infrastructural development of the labor market, which led to the emergence of new forms of organization of labor activity – self-employment and platform employment. The paper determines that the introduction of a special tax regime and a simplified registration procedure contributed to the fact that self-employment has become one of the most dynamically developing institutions in Russia. It was revealed that despite the fact that the regulation of relations between platforms and the self-employed in the legal field has certain difficulties, platform employment plays a positive socio-economic role in society.

Keywords: Self-employment, Platform employment, Special tax regime, Digital platforms, Digital technologies, Digital transformation, Labor market

Введение. Экономика многих стран переживает турбулентность, а рынки труда претерпевают структурные изменения, появляются новые формы занятости и организации трудовой деятельности, которые сосуществуют с традиционными. Для новых форм занятости характерны такие особенности, как непродолжительность контрактов, взаимодействие посредством цифровых платформ, изме-

нение места организации и осуществления трудовой деятельности. Некоторые изменения связаны с переопределением форм занятости на стыке занятости и самозанятости.

Появление новых форм занятости связано с глобальными тенденциями: цифровизацией и цифровой трансформацией экономики. В последние десятилетия цифровые технологии укоренились в самых разных отраслях экономики: торговле, туризме, транспорте. Информационно-коммуникационная революция и развитие Интернета стимулировали появление новых форм бизнеса, производственных процессов и продуктов, цифровых платформ [5. С. 1491–1506]. Цифровые экосистемы коренным образом изменили способ организации труда и бизнеса и благодаря сетевым эффектам стали основой взаимодействия заказчиков и исполнителей, модифицируя и перераспределяя трудовые ресурсы наиболее эффективным образом [10]. Поэтому не считается с тем влиянием, которое цифровые платформы оказывают на трудовые отношения и структуру рынка труда, да и на всю экономику, невозможно.

Понятие «самозанятые граждане». Прежде чем анализировать роль электронных платформ, надо определиться, с какой формой трудовых отношений мы имеем дело. На сегодняшний день российским законодательством предусмотрены: трудовой договор, гражданско-правовая сделка и работа на себя. Сегодня именно самозанятые – основной элемент платформенной занятости. Режим самозанятости рассматривается как налоговый режим, поэтому вопрос о регулировании отношений платформ с самозанятыми и легализация отношений в нормативно-правовом поле не пойдет по классическому сценарию трудового законодательства. Сложившийся формат сотрудничества не укладывается в традиционные отношения и имеет специфические особенности.

Понятие самозанятости появилось в российском законодательстве в 2017 г. Пунктом 1 статьи Гражданского кодекса Российской Федерации предусмотрено право осуществлять предпринимательскую деятельность без образования юридического лица при условии регистрации в налоговых органах. Налоговый кодекс Российской Федерации (далее – НК РФ) также определяет условия получения статуса самозанятого гражданина (пункт 7.3. ст. 83): отсутствие статуса индивидуального предпринимателя; оказание услуг другим физическим лицам (личные, домашние нужды); регистрация в налоговых органах по месту жительства или пребывания; уведомление налоговых органов о начале и прекращении деятельности.

Также пункт 70 ст. 217 НК РФ определяет круг лиц, кто может быть отнесен к категории самозанятых граждан:

- лица, осуществляющие присмотр и уход за детьми, больными, и престарелыми, которые нуждаются в постоянной посторонней помощи по решению медицинской комиссии (например, сиделки и няни);
- лица, осуществляющие уборку помещений и предоставляющие услуги по ведению домашнего хозяйства (например, домработницы и помощники по хозяйству).

Законодательством субъектов Российской Федерации может быть разработан иной перечень видов услуг, которые могут оказывать самозанятые граждане.

Например, в Москве, к этой категории отнесены инструкторы спортивной индустрии, зооняни, операторы видеосъемок торжественных мероприятий, частные детективы, фрилансеры – графические дизайнеры и др.

Перечень видов услуг постепенно будет расширяться на фоне сокращения численности ИП и упрощенной регистрации самозанятых граждан.

Итак, самозанятыми могут стать лица, не оформляющие отношения с работодателем или осуществляющие предпринимательскую деятельность без привлечения наемных работников, чей доход не превышает 200 тыс. руб. в месяц (или 2,4 млн руб. в год).

В 2019 г. в четырех регионах (в Москве, Республике Татарстан, Московской и Калужской областях) стартовал экспериментальный налоговый режим для самозанятых граждан, который сейчас охватил все остальные субъекты России. Особенность режима – уплата налога в размере 4 % за услуги физлицам и 6 % при работе с юридическими лицами вместо 13 % подоходного налога (НДФЛ). Регистрацию в качестве самозанятого можно пройти в приложении «Мой налог», а также через Единый портал госуслуг.

Оценка рынка самозанятых граждан в России. В связи с последними законодательными инициативами и установлению специальной системы налогообложения для самозанятых перед государственными органами стоит задача по оценке и выявлению граждан, подпадающих под утвержденные «критерии самозанятого населения». Возникает вопрос о количестве и методике подсчета.

Министерство труда и налоговая служба являются основными государственными органами, собирающими данные о количестве самозанятых граждан в России. Наиболее заинтересованными в информации о количестве самозанятых в России и основными государственными органами, собирающими данную статистику, являются Федеральная налоговая служба, Министерство труда и Министерство экономического развития [2. С. 553–554].

Основные методы, применяемые для сбора информации:

- проверка банковских транзакций;
- сопоставление полученных доходов и произведенных расходов;
- контрольные закупки товаров на специальных сайтах;
- мониторинг социальных сетей самозанятых граждан на предмет рекламы

услуг.

Некоторые из перечисленных методов трудоемки и неоднозначны.

Кроме государственных структур данные о количестве самозанятых собирают различные научные институты и социологические службы, но применяемые ими сугубо социологические методы могут давать статистику в несколько раз отличающуюся от официальной.

Единого ответа на вопрос сколько же в нашей в нашей стране самозанятых дать не представляется возможным. По разным оценкам в России насчитывается от 2,4 до 17 млн самозанятых граждан (табл. 1).

Таблица 1

Количество самозанятых граждан в России по различным оценкам

Организация	Оценка количества самозанятых
Федеральная налоговая служба	5,2 млн чел.
Выборочное обследование Росстат	4,9 % от экономически активного населения в возрасте 15–72 лет (около 3,5 млн чел.)
Организация экономического сотрудничества и развития	6,7 % от общего количества занятого населения
Портал социологических данных РАНХиГС	22,4 % от экономически активного населения (около 16–17 млн чел.)
Всемирный банк	2,7–7,5 млн чел.
Институт государственного и муниципального управления НИУ ВШЭ	8 млн чел.

Источник: <https://www.hse.ru/news/expertise/442785638.html>

Согласно данным Федеральной налоговой службы, число самозанятых постоянно растет. Прирост зарегистрированных самозанятых в 2022 г. в среднем колеблется от 30 до 40 % по сравнению с аналогичным месяцем 2021 г. Так в июне 2021 г. количество самозанятых составляло 2,5 млн чел., а в июне 2022 г. – 5,2 млн чел. (рис. 1). В 2022 г. ежедневно в качестве самозанятых регистрируются около семи тысяч человек. По прогнозным оценка количество зарегистрированных самозанятых к 2024 г. может увеличиться до 8,4 млн чел., а к 2030-му – порядка 10–11 млн.

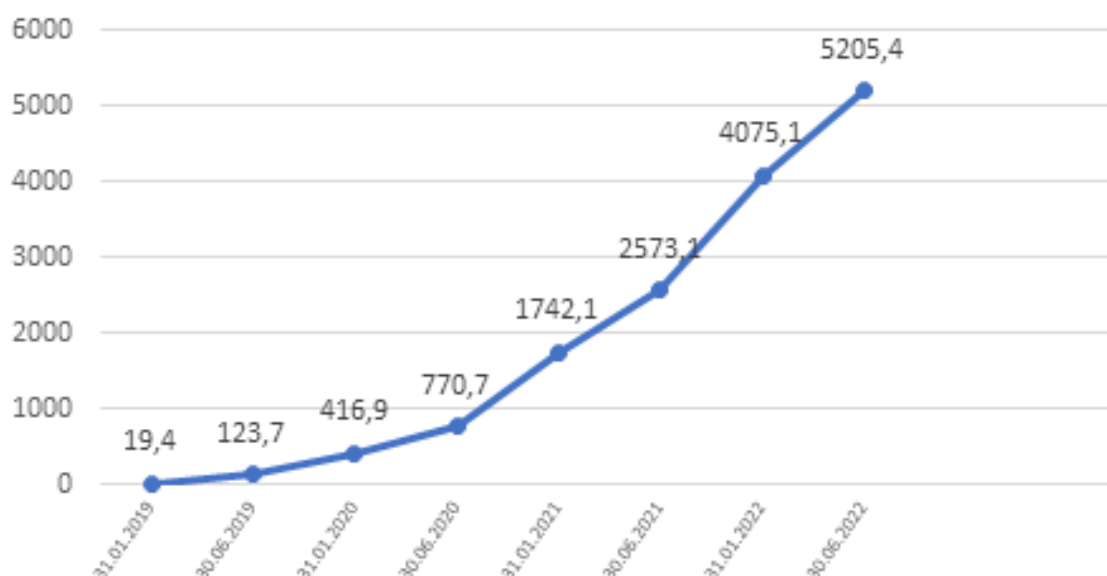


Рис. 1. Количество самозанятых в России по данным Федеральной налоговой службы в 2019–2022 гг., тыс. чел.

Больше всего самозанятых в Москве и Московской области, Санкт-Петербурге, Краснодарском крае, Республике Татарстан, Свердловской области (рис. 2).



Рис. 2. Топ-10 регионов России по количеству самозанятых на июль 2022 г. по данным Федеральной налоговой службы, чел.

Также по данным ФНС на начало 2022 г. за весь период действия специального налогового режима суммарные доходы самозанятых превысили 882 млрд руб., сумма уплаченного дохода – 31 млрд руб., количество сформированных чеков – 610 млн сумма среднего чека – 1 446 руб. Самые популярные отрасли деятельности: ремонт, такси, IT-сфера, индустрия красоты, информационные услуги, уборка и домашнее хозяйство, обучение.

Самые высокие доходы на одного самозанятого зафиксированы в Москве, Московской области, в Татарстане и в Санкт-Петербурге.

На сегодняшний день самозанятость – это один из самых динамично развивающихся институтов в России. Столь высокая популярность и востребованность данного режима объясняется бесплатной и удобной регистрацией, низкой налоговой ставкой, минимумом отчетности, легализацией самозанятыми доходов и отсутствие рисков наложения штрафа за незаконную предпринимательскую деятельность, государственная поддержка наравне с МСП [9. С. 172–183]. Безусловно, существуют и проблемные вопросы: пенсионное обеспечение самозанятых, предоставление патентов, система администрирования налога [8. С. 979–992]. Тем не менее, формируется самостоятельный рынок труда, который требует грамотного регулирования.

Роль цифровых платформ. По разным оценкам специалистов, к 2030 г. не менее 10 млн самозанятых в России будут «платформенно-занятыми». То есть свой

труд и свой заработок они будут доверять цифровым платформам, которые, по сути, станут их работодателями. Правильное развитие «платформенной занятости» в нашей стране – это прогресс, который в будущем даст России мощное конкурентное преимущество на международном рынке труда.

Для самозанятых онлайн-платформы – основной канал поступления работы и заказов, выступая в качестве медиаторов и фасилитаторов процесса оказания услуг (рис. 3).

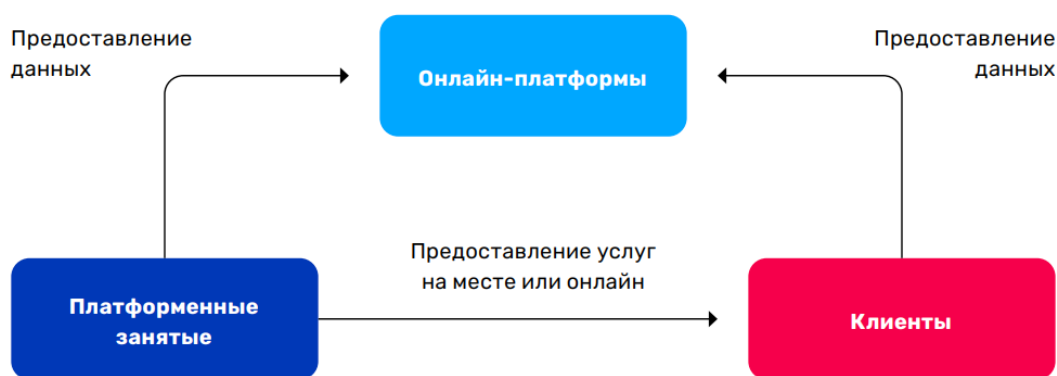


Рис. 3. Взаимодействие при платформенной занятости

Таким образом, самозанятость посредством платформ – это простой и эффективный способ получения регулярного или эпизодического дохода. Развитие платформенной инфраструктуры позволяет избежать транзакционных и административных издержек, дает возможность самозанятым выйти за рамки традиционной организации труда по найму, оптимизировать процесс профессионального развития и роста. Платформенная занятость видоизменяет архитектуру рынка труда, увеличивая его гибкость и расширяя возможности его участников [3, 7].

Низкие барьеры входа, гибкий график, дистанционный формат делают платформенную занятость привлекательной для самых разнообразных категорий граждан от профессионалов до маломобильных и социально-уязвимых категорий. Это формирует каналы инклюзии для молодежи без опыта работы, лиц предпенсионного и пенсионного возрастов, многодетных матерей и матерей с малолетними детьми, лиц с ограниченными возможностями здоровья, способствуя росту их доходов и снижению нагрузки на системы государственной социальной поддержки.

Развитие платформенной занятости увеличивает число поставщиков бытовых и цифровых услуг, стимулирует расширение сегмента малых и средних предприятий в различных отраслях, тем самым ускоряя развитие экономики в целом. Цифровые платформы способствуют «обелению» экономики за счет «вывода из тени» части экономической деятельности и занятости и переводу из неформального сегмента в поле самозанятости.

Оборотная сторона платформенной занятости – риск прекаризации рабочей силы, который обусловлен отсутствием минимального уровня стоимости услуг, социальной незащищенностью в период временной нетрудоспособности, а также провоцированием избыточной и интенсивной занятости, вызывающей переутомление.

Из этого следует, что эта новая экономика определяет благополучие миллионов граждан и обеспечивает продуктами и услугами десятки миллионов россиян. Когда мы говорим о таких масштабах «платформенно зависимых» людей, очень важно помнить об их интересах. Здесь важно соблюсти баланс, а именно не забыть об интересах бизнеса и цифровых платформ, учесть потребности тех, кто хочет быть платформенно занятым и тех, кто получает товары и услуги благодаря работе платформ и занятых на них.

На рынке представлены тысячи сервисов для бизнеса, которые подходят для самозанятых предпринимателей (табл. 2).

Таблица 2

Цифровые сервисы для самозанятых

Платформы информационной поддержки	Платформы для поиска работы	Специализированные платформы
<ul style="list-style-type: none"> - Самозанятые.рф - npd.nalog.ru - tvoedelo.pro 	<ul style="list-style-type: none"> - Универсальные - YouDo - Profi.ru - uslugi.yandex - Kwork - FL.ru - HeadHunter 	<ul style="list-style-type: none"> - Мастерплейс - superbuh24.ru - Illustrators. Ru - Правовед.Ру - Мой налог - ЮSelf - Qugo.ru - СберУслуги - Яндекс.Про. и др.
Сервисы для продажи товаров	Доски объявлений	
<ul style="list-style-type: none"> - Онлайн-ритейлеры - Wildberries - Ozon 	<ul style="list-style-type: none"> - Авито, Юла и др. - Ярмарка мастеров 	

Цифровые платформы по поиску и предоставлению услуг популярны среди пользователей, ежемесячно их посещают около 20 млн чел. и заключается около 15 млн сделок. Данные по работе отдельных платформ представлены в табл. 3. Основные формы монетизации платформ: комиссии со сделки, плата за положительные отклики и за продвижение исполнителей, плата за размещение заказов.

Таблица 3

Статистические показатели отдельных цифровых платформ

Платформа	Количество посетителей сайта (в месяц)	Количество зарегистрированных пользователей		Количество заключаемых сделок
		Всего	Исполнителей	
Profi.ru	5 680 000		1 000 000	7 728 156
Правовед	5 380 000		35 321	
Text.ru	1 878 682			
Youdo	1 750 000	7 000 000	2 000 000	7 547 872
FL.ru	1 520 000		1 000 000	
Kwork	1 278 527	2 000 000		
eTXT	1 150 000	1 500 000	1 000 000	

Новые инструменты цифровых платформ предоставляют дополнительные возможности для самозанятых. Так, электронная площадка «Мои самозанятые» для взаимодействия компаний и фрилансеров запустила сервис, позволяющий подписывать юридически значимые документы в Telegram без установки специальных приложений.

YouDo и HeadHunter запустили цифровой сервис «YouDo Бизнес» для работы с самозанятыми и юридическими лицами летом 2021 г. HeadHunter планирует инвестировать в нее еще 5 млн долл. и сделать лидером рынка подработки. «YouDo Бизнес» оказывает услуги по постановке на учет и передаче прав в Федеральную налоговую службу, формированием чеков, уплатой налогов и документооборотом, HeadHunter осуществляет маркетинговое продвижение и услуг клиентам.

Хотя ФНС уже предоставляет сервис («Мой налог») для самозанятых, в «Сбере» также решили использовать инструмент (ЮSelf) в рамках своей платежной системы ЮMoney. Основное преимущество – интеграция учета доходов с другими платформами для фрилансеров и оплата услуг онлайн. Личный кабинет ЮSelf можно использовать для постановки на учет в налоговой, формирования чеков, уплаты налогов, получения уведомлений и налоговых расчетов. Начисление налога на сервисе осуществляется только по зарегистрированным чекам.

Так же «Сбер» предлагает сервис «СберУслуги» для размещения услуг у самозанятых. Все исполнители проходят регистрацию и идентификацию через «Сбер ID» и оплачивают комиссию – не более 10 % от суммы каждой совершенной сделки. Заказчики могут ознакомиться с профилем специалистов, отзывами и ценами. Сервис формирует рейтинг исполнителей на основе отзывов и оценок заказчиков, которые уже воспользовались услугами. По результатам сделки формируется чек, который получает заказчик. Заказчикам и исполнителям обеспечивается гарантия сделок за счет страховых продуктов «Сбера». Аналогичные услуги предлагают и другие платформы, например, YouDo, Profi.ru, Remontnik.ru.

«Маркетплейс» для самозанятых Qugo.ru позволяет компаниям находить исполнителей, а самозанятым – заказчиков. Сервис ориентирован на такие сферы как курьерские услуги, ремонт, строительство, складские и логистические операции, клининг, рекрутинг и т. д. Платформа обеспечивает документооборот, автоматизацию финансовых и фискальных процессов, планирование задач, отбор исполнителей по установленным критериям.

«Яндекс» модифицировал приложение «Таксометр», теперь оно называется «Яндекс.Про», приспособив его для различных категорий самозанятых (водителей, курьеров, мастеров). Приложение предоставляет услуги по регистрации в качестве самозанятого и синхронизации данных с приложением ФНС России «Мой налог», для автоматизации перечисления платежей и налогов, также можно осуществлять поиск заказов в различных сервисах «Яндекса» («Яндекс.Услуги», «Толока», «Лавка»). Выплаты можно получать на заранее привязанную банковскую карту.

Для большинства самозанятых платформенная занятость является временной. Исполнители больше всего ценят возможность работать с разными платформами и самостоятельно планировать время. С 2019 г. маркетплейсы активно привлекают самозанятых.

За счет сотрудничества с самозанятыми онлайн-магазины увеличивают прибыль; расширяется ассортимент товаров ручной работы, появляются уникальные и необычные товары, которые пользуются спросом и которые нельзя найти в обычных магазинах, тем самым увеличивается поток покупателей; в некоторых случаях отсутствует необходимость заключения постоянных договоров найма; сокращаются сроки и расширяются возможности курьерской доставки в отдаленных и малочисленных населенных пунктах; снимается часть налоговой нагрузки (заключение договоров подрядов и индивидуальными предпринимателями и юридическими лицами обходится дороже, чем работа с самозанятыми); сокращается объем документооборота (чек в обработке проще, чем счета); увеличивается доход с комиссий.

Но сотрудничество взаимовыгодно для обеих сторон. Самозанятым онлайн-маркеты предоставляют возможность осваивать сетевой рынок, расширяя географию и объемы продаж во всех регионах присутствия без расходов на рекламу и продвижение. Например, регистрация и заполнение карточки в сервисе Ozon предоставляет доступ к миллионам покупателей по всей России, а рекламу и доставку берет на себя интернет-магазин. Крупные маркетплейсы предоставляют свою готовую клиентскую базу, сильный бренд, обеспечивая прямой доступ к потоку лояльных клиентов. Онлайн-платформы постоянно работают над расширением клиентской базы и продвижением площадки, что является весомым плюсом для самозанятых.

Онлайн-площадки предоставляют широкий набор инструментов для продаж. Не нужно самостоятельно создавать лендинг, заниматься продвижением в соцсетях, тратиться на прямую рекламу. Многие сетевые ритейлеры оказывают консультативную и технологическую поддержку на этапе подключения и ознакомления с работой на платформе, ее особенностями, инструментами продвижения товаров и услуг, заполнением карточек товаров. Проводятся семинары экспертов по интернет-продажам.

При работе с маркетплейсами самозанятые получают доступ к выстроенной логистической инфраструктуре: складам, системам доставки и пунктам выдачи товаров, контакт-центрам и т. д. Это позволяет локальному бренду избежать дополнительных издержек и выйти за ограниченные рамки своего города и региона.

Но, безусловно, есть и ограничения при работе с онлайн-платформами: соблюдение правил маркетплейсов; работа в законодательном поле и установленных границах для налогового режима самозанятых; соблюдение правил маркировки и сертификации продукции; технологические трудности.

Заключение. Несмотря на то, что самозанятость посредством цифровых платформ является новой формой трудовых отношений, которые не попадают под традиционное нормативное правовое регулирование, ряд экспертов подчеркивают ее позитивную социально-экономическую роль в повышении доходов населения, сокращении неформальной занятости и безработицы среди социально-уязвимых категорий граждан и поддержки жителей депрессивных регионов и моногородов [4]. А введение экспериментального налогового режима [1. С. 8–16; 6. С. 131–140], стремление платформ к обеспечению информационной прозрачности стимулировали детеневилизацию существенной части услуг и сокращение незаконной предпринимательской деятельности.

Список литературы

1. Абрамова Е. А. Налоговой спецрежим для самозанятых в Российской Федерации: преимущества и спорные вопросы // Современные наукоемкие технологии. Региональное приложение. 2021. № 1 (65). С. 8–16.
2. Агабекова Б. Ф., Боркова Е. А., Короткова П. Д. Анализ методов контроля и регулирования деятельности самозанятых граждан в РФ // Экономика труда. 2019. Т. 6. № 1. С. 553–564.
3. Бобков В. Н., Черных Е. А. Платформенная занятость: масштабы и признаки неустойчивости. Мир новой экономики. 2020. № 14 (2). С. 6–15.
4. Бобков В. Н., Одегов Ю. Г., Гарнов А. П. Регулирование неустойчивой занятости в моногородах // Экономика региона. 2020. Т. 16, вып. 2. С. 522–534.
5. Волкова А. С., Константинова Д. С., Кудаева М. М., Масалова Ю. А. Изменение подходов к использованию человеческих ресурсов под воздействием цифровых технологий // Креативная экономика. 2020. Т. 14, № 8. С. 1491–1506.
6. Гончаренко Л. И., Адвокатова А. С. Налог на профессиональный доход: риски и потенциал // Экономика. Налоги. Право. 2020. № 5. С. 131–140.
7. Петровская Н. Е. Цифровые платформы как доминантный вектор развития глобального рынка труда // Управление. 2021. Т. 9, № 2. С. 103–113.
8. Скруг В. С. Возможности и проблемы легализации самозанятых в условиях цифровой экономики // Экономика труда. 2020. Т. 7, № 11. С. 979–992.
9. Тонких Н. В., Бабинцева А. В. Исследование самозанятости населения в Российской Федерации: общие и частные проблемы // Вестник ОмГУ. Серия: Экономика. 2020. № 1. С. 172–183.
10. Berg J., Furrer M., Harmon E., Rani Uand M. S. Silberman. Digital Labour Platforms and the Future of Work: Toward Decent Work in the Online World. International Labour Organization, Geneva, 2018. URL: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_645337.pdf (дата обращения: 17.08.2022).

В. В. Генюш,
студент,

Гродненский государственный университет имени Янки Купалы

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ВОПРОСЫ ЦИФРОВИЗАЦИИ ДОКУМЕНТООБОРОТА В ЮРИДИЧЕСКОЙ КЛИНИКЕ

Аннотация. В статье анализируются вопросы практического применения инструментов legal tech в работе юридических клиник. При этом указываются области применения, и актуализируется потребность в обучении студентов-юристов не только цифровым компетенциям, но и эффективным способам их использования для решения правовых задач. Юридическое клиническое образование способствует овладению новыми информационными технологиями и содействует профессиональной подготовке юристов нового поколения. Сделанные выводы основаны на личном опыте работы в Юридической клинике Гродненского государственного университета имени Янки Купалы (ГрГУ имени Янки Купалы). В ходе изложения

материала дается краткий обзор применяемых цифровых технологий, отмечается их способность и инструментарий по использованию в делопроизводстве и документообороте юридических клиник. Практическая значимость и новизна статьи заключаются в оценке использования цифровых технологий на примере деятельности Юридической клиники ГрГУ имени Янки Купалы, анализе рационализации юридической деятельности с учетом использования инструментов legal tech и с учетом рисков современной информационной среды.

Ключевые слова: право, цифровые технологии, юридическая клиника, legal tech, документооборот, делопроизводство, цифровизация

ORGANIZATIONAL AND LEGAL ISSUES OF DIGITALIZATION OF DOCUMENT FLOW IN A LAW CLINIC

Abstract. The issues of practical application of legal tech tools in the work of legal clinics are analyzed in the article. At the same time, the areas of application are indicated and the need for training law students not only in digital competencies, but also in effective ways of using them to solve legal problems is actualized. The author believes that legal clinical education contributes to the mastery of new information technologies and contributes to the professional training of new generation of the lawyers. The conclusions made by the author are based on personal experience in the Legal Clinic of the Grodno State University named after Yanka Kupala. In the course of presenting the material, the author gives a brief overview of the digital technologies that have been used, notes their ability and tools for use in office work and workflow of legal clinics. The practical significance and novelty of the article lies in the assessment of the use of digital technologies on the example of the activities of the Legal Clinic of the Yanka Kupala State University, the analysis of the rationalization of legal activities, taking into account the use of legal tech tools and taking into account the risks of the modern information environment.

Keywords: Law, Digital technologies, Law clinic, Legal tech, Document management, Office work, Digitalization

Усвоение студентами-юристами основ делопроизводства и документооборота – одно из важнейших условий их профессионального развития и вовлеченности в работу. От того, насколько внимательно изучены и правильно составлены документы, как организована работа с ними, во многом зависит своевременность и обоснованность готовых правовых решений с учетом рисков. А как сформировать практические навыки ведения делопроизводства у студента юридического факультета?

На наш взгляд, одним из эффективных способов подготовки молодого специалиста к практической деятельности юриста является дополнительное клиническое образование.

Юридическое клиническое образование реализуется через юридическую клинику (далее – ЮК) – подразделение высшего учебного заведения (факультета), создаваемое с целью обучения студентов-правоведов практическим навыкам [7. С. 231].

Юридическая клиника – это один из социально ориентированных проектов в юридическом образовании, который помогает студентам-клиницистам осознать

реальную сущность и роль юриста в обществе, овладеть профессиональной этикой, получить практический опыт работы в части оказания бесплатной юридической помощи населению, участвовать в правовом просвещении граждан [4. С. 512].

На базе Гродненского государственного университета имени Янки Купалы на протяжении более 20 лет функционирует Юридическая клиника (далее – ЮК ГрГУ). В ЮК ГрГУ функционируют такие основные направления деятельности, как правовое консультирование граждан, правовое просвещение и специальное направление – паллиативная юридическая помощь.

В процессе реализации функций ЮК ГрГУ студенты-клиницисты сталкиваются со следующими задачами делопроизводства: 1) обеспечение своевременной (составление проектов правовых документов в установленный правилами ЮК ГрГУ срок) и правильной (соответствие содержания проектов правовых документов нормам актуального материального и процессуального законодательства) подготовки документов; 2) организация работы с документами (выбор необходимого инструментария для создания документа и распределения обязанностей по его созданию между студентами-клиницистами); 3) создание образцов и примеров юридической документации для использования в справочных целях; 4) выполнение определенного цикла операций с документами (получение, обработка, систематизация, контроль, хранение).

Сегодня делопроизводство в ЮК ГрГУ подразумевает, что студенты совместно с кураторами:

1) осуществляют подготовку проектов документов для клиентов – обращений (заявления, жалобы), исковых заявлений, ходатайств и т. д.;

2) ведут документооборот – регистрируют обращения клиентов в ЮК ГрГУ, составляют личные карточки клиента, собирают копии предоставленных правовых документов клиентами, систематизируют документы, которые появляются вследствие работы по кейсу (например, ответы на обращения гражданина, судебные решения и т. д.). С учетом вступления в силу Закона «О защите персональных данных» кураторы ЮК ГрГУ дополнительно разработали формы для получения согласия клиента на обработку персональных данных, где отражены цель использования персональных данных, срок использования и условия использования;

3) организуют хранение документов в соответствующей привязке к делам;

4) ведут учет документов с момента их создания или поступления путем распределения дел по папкам. Для быстрого поиска нужного документа каждый кейс имеет дату, наименование и краткое содержание обстоятельств. На протяжении долгого периода в ЮК ГрГУ существовал лишь бумажный документооборот, а в качестве классификации документов использовалась группировка их в отдельные кейсы и размещение в тематические папки. А для хранения информации был создан журнал приема граждан и бумажные варианты документов, хранящиеся в сейфе. Такая достаточно понятная и легкая в использовании номенклатура дел дает возможность найти необходимый документ. Среди плюсов данной организации документооборота можно отметить его доступность (для хранения бумажных документов не нужно покупать компьютеры), безопасность (гарантия от компьютерного взлома, недопущение несанкционированного исправления).

Но, несмотря на довольно очевидные преимущества бумажного документооборота, недостатков у него больше:

- длительные сроки подготовки и согласования документов, медленный поиск документов и их содержимого, трудности при отслеживании актуальности использованных нормативно-правовых актов,
- трудности отслеживания документа на всех этапах его жизненного цикла,
- сложность организации документооборота, если с одними и теми же документами работает сразу несколько студентов,
- привязка к месту, где хранятся документы, т. е. невозможность онлайн-работы с документами [1. С. 4–6].

В итоге назревала необходимость: 1) повысить оперативность нахождения и обработки документов, 2) создания возможности работать онлайн с документами, 3) совершенствования механизма совместной работы с документами студентов и кураторов ЮК ГрГУ, 4) хранения огромного массива информации в виде нормативно-правовых документов, 5) обретения возможности быстрого поиска документов, выбора заданных параметров.

Одним из таких решений стало использование информационных технологий в деятельности ЮК ГрГУ.

В условиях пандемии COVID-19 студенты и кураторы ЮК ГрГУ, помимо привычных офлайн-консультаций, применяли онлайн-способы интервьюирования и консультирования граждан посредством видео-конференц-связи, что позволило перейти на иной уровень общения с клиентами. Сегодня студенты и кураторы ЮК ГрГУ продолжают активно использовать с учетом рисков профессиональные инструменты Legal tech. Среди наиболее часто используемых хотелось бы выделить: правовой поиск по ключевым словам, выборка судебных решений в справочных правовых системах (ЭТАЛОН, КонсультантПлюс, Пех), комментарии специалистов в области права по нововведениям в законодательство и доктринальные подходы к различным правовым вопросам (Cyberleninka, eLIBRARY), использование приложений для видеоконференцсвязи (Zoom, Webex, Discord) с целью обсуждения и проработки деталей фактов и правовых тренингов, использование Google Документы для совместного редактирования текста, сервис Kahoot, Quizzizz для интерактивного способа донесения информации слушателям в рамках правового просвещения граждан и другие [3. С. 46–47].

Внедрение цифровых технологий в деятельность ЮК ГрГУ помогло также усовершенствовать и улучшить процесс ведения делопроизводства и документооборота. Так, например, появилась возможность использовать готовые образцы документов, составленных по состоянию актуальных нормативно-правовых актов (ЭТАЛОН, «КонсультантПлюс», Пех), сравнивать один и тот же правовой документ по форме и содержанию для различных юридических обстоятельств, при этом экономя время. Также на правовых порталах можно ознакомиться с содержанием последних изменений в законодательстве, поэтому отпадает необходимость в «настольных распечатках» некоторого законодательства и корректировке кодексов на бумажных носителях.

Благодаря развитию социальных сетей ЮК ГрГУ кураторам и студентам удается быть на связи 24/7 без привязки к рабочему кабинету, что благоприятно

сказывается на решении правовых кейсов и приводит к скорейшему формированию консультации для клиента. Также посредством мессенджеров (Telegram) стал удобнее обмен внутренними документами с учетом мер безопасности и защитой персональных данных. С помощью функции создания бесед в социальных сетях можно сформировать рабочую группу по подготовке консультации для клиента и актуализировать информацию во вложениях, а название беседы можно приурочить к названию кейса, что потенциально улучшает поиск при необходимости дополнительно ознакомиться с деталями кейса. Используя приложение Zoom для проведения интервьюирования и консультирования клиентов онлайн, с их согласия мы можем вести запись встречи, что также упрощает работу при подготовке правовых ответов и способствует совершенствованию качества интервьюирований и консультаций.

Применение в работе ЮК ГрГУ таких инструментов как Google Документы и Google Диск обеспечило подготовку правовых консультаций в более короткие сроки, качественно улучшив работу над кейсом. Так, появилась возможность открыть доступ к документу конкретным студентам ЮК ГрГУ только для просмотра содержания, т. е. для ознакомления с фабулой и предложенными правовыми решениями в образовательных целях. Для кураторов ЮК ГрГУ просмотр документов с возможностью оставлять комментарии позволил вносить правки и направлять студентов на изучение дополнительной литературы, правовых источников, правоприменительной и судебной практик.

При совместной работе над документом в режиме онлайн всегда можно видеть иконки пользователей, одновременно работающих с файлом, а также есть возможность устроить обсуждение документа, нажав на кнопку чата. Такая функция помогает оценить работу каждого клинициста, участвующего в подготовке консультации и объединить результаты в совместном документе, а также совместно обсудить детали проработки и спорные моменты по фабуле дела. После добавления комментария к документу студентом-клиницистом, иконка с пометкой будет отображаться на полях до тех пор, пока не будет отмечена как решенная, что позволяет увидеть точку зрения каждого участника обсуждения и выработать совместное командное решение с учетом рисков. Помимо иконок сверху экрана действия каждого участника над документом также отображаются в реальном времени. Можно увидеть где именно находится курсор того или иного пользователя, а также те действия, что он производит – ввод или удаление текста, редактирование и многое другое. Рядом с курсором каждого коллеги отображается его имя. Это позволяет грамотно распределить работу между студентами и избегать выполнения одной и той же технической работы несколькими клиницистами, что экономит время.

Нельзя не отметить, что работать с документами можно с самых разных устройств, поэтому у студентов нет привязки к рабочему месту и они могут участвовать в обсуждении документа/ его редактировании со своего смартфона. Избежать потерь проработанной информации и удаления документа из-за некорректной работы устройств помогает автосохранение документа.

По итогам работы документ с консультацией и иные документы, относящиеся к фабуле дела, загружаются на GoogleДиск. Осознавая, что мы имеем дело с кон-

фиденциальной информацией о клиентах, мы максимально защищаем настройки конфиденциальности своей учетной записи Google посредством включения двухфакторной аутентификации, чтобы расширить дополнительный уровень безопасности документов и ресурсов [5].

Также хотелось бы обратить внимание, что с использованием цифровых инструментов удалось решить проблему длительного согласования документов (любой документ, подготовленный студентом-клиницистом, тщательно проверяется куратором, дипломированным юристом), стало возможным работать в команде с документами онлайн, а также усовершенствовался процесс хранения документов. Благодаря справочно-поисковым системам решился вопрос медленного поиска актуальных правовых документов и законодательства, стало возможным искать необходимые законы и процессуальные документы по выбору заданных параметров.

В целом необходимо отметить, что цифровизация юридического клинического образования заключается не только в оцифровке документооборота, учебников, учебных материалов и доступе к скоростному Интернету [9. С. 173]. Она выражается в дополнительном, неограниченном доступе к информационным системам, позволяющим клиницистам и кураторам получать доступ к образовательным ресурсам с любых устройств, независимо от места нахождения и времени суток. Использование цифровых инструментов в практической деятельности показывает, насколько порой теоретическая база без должной практической подготовки может тормозить процесс обучения и развития новых профессиональных навыков юриста. Внедрение legal tech дополнительно мотивирует восполнять недостаточность фундаментальных исследований, специальной, учебной и методической литературы для подготовки юриста цифровой [8. С. 28–29].

Тем не менее, использование цифровых технологий должно быть обосновано и действительно необходимо в работе юридической клиники. Основная задача цифровизации образования – повышение результативности процесса обучения, а не слепое следование «тренду» [2]. При этом мы понимаем те возможные риски, которые могут возникнуть по применению цифровых технологий, и солидарны с А. А. Кулаковой и В. С. Манохиным, что «современному юристу необходимо не только уметь пользоваться новыми технологиями, но и понимать их природу, какие риски они в себе заключают и как с точки зрения законодательства правильно их рассматривать» [6. С. 196].

Таким образом, внедрение цифровых технологий в организацию учебного процесса, использование преимуществ цифровизации (доступность информации, новые онлайн приложения для работы с клиентами) привели к постепенным и качественным изменениям в работе юридической клиники. Благодаря мастерству и профессионализму кураторов ЮК ГрГУ, студентам удалось не просто быть на волне информационно-коммуникативных технологий, но и эффективно реализовывать дополнительные возможности по освоению профессиональных навыков юриста [2].

Стоит отметить, что, несмотря на широкую автоматизацию юридической деятельности посредством инструментов legal tech, поиск новых возможностей применения информационных технологий продолжается. Ведется работа по совер-

шенствованию организации документооборота в ЮК ГрГУ, в частности, длительному хранению наработанных практических материалов. Направлениями для развития цифровых навыков клиницистов при работе с фабулами выбраны: внедрение технологий мобильного доступа, разработка собственных онлайн-проектов, защита информации от несанкционированного доступа, изучение эффективных технологий хранения и воспроизведения электронной информации.

Список литературы

1. Асланьянц Н. Л. Документационное обеспечение управления юридической фирмой ООО «протокол справедливость» в условиях цифровой трансформации // Практика 2021: документоведение, архивоведение, менеджмент: материалы заключительной научно-методической конференции «Практика2021» по подведению итогов практик, проведенных в 2021 г. по кафедре общего, стратегического, информационного менеджмента и бизнес-процессов КГУ. Краснодар, 17–20 декабря 2021 года. Краснодар: Кубанский государственный университет, 2022. С. 3–8.

2. Генюш В. В. Опыт Юридической клиники ГрГУ имени Янки Купалы по внедрению цифровых технологий в образовательную деятельность // Материалы Международного молодежного научного форума «ЛОМОНОСОВ-2022» / отв. ред. И. А. Алешковский, А. В. Андриянов, Е. А. Антипов, Е. И. Зимакова. Москва: МАКС Пресс, 2022. URL: https://conf.msu.ru/archive/Lomonosov_2022/data/info.htm (дата обращения: 05.08.2022).

3. Генюш В. В. Профильные навыки, приобретаемые молодым юристом при получении дополнительного клинического образования // Леденцовские чтения. «Бизнес. Наука. Образование». Правовые и экономические аспекты: сборник материалов X Международной научно-практической конференции (г. Вологда, 28 апреля 2022 года) / Союз Вологодская торгово-промышленная палата, Вологодское областное потребительское общество, Вологодский кооперативный колледж, Северо-Западный институт (филиал) Университета имени О. Е. Кутафина (МГЮА); ответственный редактор Ю. А. Пеганова. Вологда: Северо-Западный институт (филиал) Университета имени О. Е. Кутафина (МГЮА), 2022. С. 43–47.

4. Генюш В. В. Юридическая клиника как один из важных проектов в становлении молодого специалиста // Осенние чтения «Молодежь и право»: материалы I Междунар. науч. конференции студентов, магистрантов и аспирантов, Минск, 19 ноября 2020 г. / БГУ, Юридический фак.; [редкол.: А. А. Пухов (отв. ред.) и др.]. Минск: БГУ, 2021. С. 512–513.

5. Компьютерная грамота. Совместная работа с документами Google – 2016. Сентябрь. URL: <https://pcgramota.ru/portfolio/sovmestnaya-rabota-s-dokumentami-google> (дата обращения: 17.08.2022).

6. Кулакова А. А. Цифровое право как учебная дисциплина: целесообразность введения и особенности / А. А. Кулакова, В. С. Манохин // Вестник Владимирского юридического института. 2020. № 3 (56). С. 196–199.

7. Новицкая М. В. Актуальные проблемы и перспективы развития юридического клинического образования в Республике Беларусь: сборник материалов

заочной научно-методической конференции, посвященной 70-летию образования Могилевского института МВД (Могилев, май 2018 года) // Министерство внутренних дел Республики Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь»; редкол.: Ю. П. Шкаплеров (председ.) [и др.]. Могилев: Могилев. институт МВД, 2018. С. 231–236.

8. Смотров И. В. Проблемные аспекты юридической профессии в условиях развития цифровой экономики // Академия права и экономики. 2018. № 3 (7). С. 26–29.

9. Danker B. Using flipped classroom approach to explore deep learning in large classrooms / B. Danker // IAFOR Journal of Education. 2015. № 3 (1). Pp. 171–186.

Е. М. Глянц,

адвокат коллегии адвокатов Республики Татарстан
«Рыбак, Коган и партнеры»

ПРОТИВОДЕЙСТВИЕ КИБЕРМОШЕННИЧЕСТВУ: ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ

Аннотация. Целью работы является выявление проблем, возникающих при раскрытии и расследовании кибермошенничества, а также трудностей защиты прав потерпевших от этих преступлений. Исследование проведено на примере конкретного дела, в рамках которого адвокатом осуществляется защита потерпевшего. Рассматриваются негативные последствия, возникающие в результате преступления не только в рамках уголовного права, но и в гражданско-правовой плоскости. В ходе исследования были опрошены действующие сотрудники правоохранительных органов, непосредственно участвующие в раскрытии и расследовании кибермошенничеств. Выводы сделаны исходя из реальных ситуаций, возникающих на практике.

Ключевые слова: кибермошенничество, телефонное мошенничество, дистанционное мошенничество, цифровые технологии, хищение, онлайн-банкинг, дистанционное оформление кредита, виктимология

COUNTERING CYBERFRAUD: PROBLEMS OF THEORY AND PRACTICE

Abstract. The purpose of this paper is to identify the problems encountered in the detection and investigation of cyberfraud, as well as the difficulties of protecting the rights of victims of these crimes. The research is carried out on the example of a specific case, in which the lawyer defends the victim. The negative consequences arising as a result of the crime are considered not only in criminal law, but also in civil law. In addition, the study interviewed current law enforcement officers directly involved in the detection and investigation of cyber-fraud. Conclusions were made on the basis of real situations arising in practice.

Keywords: cyberfraud, telephone fraud, remote fraud, digital technology, crime victim, fraud victim, theft, online banking, remote loan processing, victimology

Мошенничество – это один самых распространенных видов хищений. С развитием информационно-коммуникационных технологий мошенничество шагнуло в киберпространство. Мошенники успешно пользуются достижениями научно-технического прогресса, совершенствуя методы совершения преступлений и способы сокрытия их следов.

Заместитель председателя Совета Безопасности Российской Федерации Д. А. Медведев неоднократно обращал внимание на рост киберпреступности, в ситуации которой особенно уязвимыми оказались физические лица. В первую очередь это касается пожилых людей. «Чтобы заполучить их денежные средства, имущество злоумышленники, действительно, действуют весьма изощренно», - заметил замглавы Совбеза, сделав акцент на том, что подавляющее большинство таких преступлений совершается с использованием современных технических средств связи и информации [8].

Российскими исследователями сформулированы факторы, способствующие совершению мошеннических действий в сфере информационно-коммуникационных технологий. Так, выделяются следующие причины:

- 1) неосведомленность граждан о возможных мошеннических посягательствах в информационно-телекоммуникационной сети;
- 2) постоянная изменчивость способов мошеннических действий в информационной среде;
- 3) правильное и качественное психологическое воздействие злоумышленника на выбранную жертву;
- 4) владение мошенником информацией о личных данных выбранного для посягательства лица, что помогает войти в доверие и ввести в заблуждение жертву;
- 5) профессионализм, хорошая конспирация мошенника при совершении преступления;
- 6) многочисленность мошеннических актов;
- 7) создание экстремальной обстановки для выбранной жертвы, доведение лица до состояния необдуманных действий и др. [6. С. 30–34]

В настоящей статье тема кибермошенничества будет рассмотрена на примере одного из его видов — так называемого телефонного мошенничества. Хотя в настоящее время его уже нельзя назвать телефонным мошенничеством в чистом виде. Скорее это дистанционное мошенничество с использованием информационных технологий (IT – мошенничество).

В современной жизни большой популярностью пользуются сервисы онлайн-банкинга, которые помогают нам мгновенно совершать финансовые операции, дистанционно заключать кредитные договоры, оплачивать кредиты и т.д.

Приложения онлайн-банкинга все чаще становятся частью мошеннических схем. С помощью приложений банков на потерпевшего дистанционно оформляются кредиты, затем кредитные средства похищаются.

Рассмотрим эту проблему на конкретном примере.

Пенсионерка Светлана Х. работает в детском саду воспитателем. В сентябре 2021 года ей позвонила девушка и представилась специалистом службы безопасности одного из республиканских банков. У потерпевшей в этом банке была зарплатная карта, также на карту этого банка она получала пенсию.

Звонившая сообщила, что в банк поступила заявка о смене номера телефона, и была произведена попытка снятия 8000 рублей с карты Светланы Х., а также была попытка оформления кредита на максимальную сумму. Девушка обратилась к Светлане Х. по имени отчеству. Звонившая успокоила потерпевшую: «Номер карты, коды и иные данные сообщать не надо. Сейчас я Вас переключу на другого специалиста. Все разговоры записываются». Это вызвало доверие у потерпевшей. Ведь ей было известно, что мошенники сразу пытаются выведать номера карты, коды и прочую конфиденциальную информацию.

После переключения ответил мужчина, представившийся специалистом службы безопасности Центробанка. Он сказал, что мошенники подали заявку на получение кредита на имя потерпевшей на крупную сумму, кредит уже одобрен. Отменить его нельзя, а чтобы деньги не ушли на счет другого человека, нужно получить деньги и поместить их на защищенные счета Центробанка.

Далее Светлане Х. поступил звонок с номера, определившегося как «Управление ФСБ России по Республике Татарстан».

Звонивший мужчина представился сотрудником ФСБ и рассказал, что в банке есть группировка сотрудников, которые продают данные клиентов и сами являются мошенниками.

После этого разговора у потерпевшей уже не оставалось сомнений в правдивости информации, сообщаемой звонившими.

Затем со Светланой Х. связался звонивший ранее «специалист службы безопасности Центробанка», но уже посредством мессенджера WhatsApp. Он прислал ей сканы своего удостоверения с фотографией. И сообщил, что вся «операция» по «спасению» ее денег будет проходить под его контролем, и она должна беспрекословно выполнять его указания.

Через несколько дней потерпевшей поступило сообщение от банка о том, что ей предоставлен кредит на сумму 850 000 рублей.

Светлана Х. сразу же позвонила на официальную горячую линию этого банка и заявила, что кредит ей не нужен, просила отменить его. Однако специалист горячей линии заявила, что отменить кредит уже невозможно.

После этого разговора потерпевшая окончательно поверила в то, что говорили ей мошенники: сотрудники банка – участники преступной схемы и им верить нельзя.

На следующий день потерпевшая сообщила об одобренном кредите «специалисту службы безопасности Центробанка». Он дал указание: срочно снять деньги и поместить их на защищенные счета. Для этого нужно ехать в Казань (потерпевшая проживает в другом городе), по пути ни с кем не разговаривать, только с ним и только посредством наушников.

Потерпевшая отпросилась с работы и поехала в Казань по указанному злоумышленником адресу. Там через банкомат она снимала кредитные средства частями и переводила их на указанные мошенником реквизиты. Возможно, посредством системы PayPass. Сама потерпевшая точно этого сказать не может, так как не разбирается в этих технологиях.

Злоумышленник убеждал потерпевшую, что с ее помощью спецслужбы разоблачат и задержат организованную преступную группу. Преступники будут наказаны, а ей будет вручена благодарственная грамота.

На электронную почту потерпевшей пришло письмо на фирменном бланке банка с печатью и подписью управляющего с тестом: «Ваш кредит погашен».

На следующий день «специалист службы безопасности Центробанка» сообщил потерпевшей, что для того, чтобы наверняка вычислить мошенников, она должна активировать имевшуюся у нее кредитную карту другого банка с кредитным лимитом 162 000 рублей. Кроме того, необходимо оформить новую кредитную карту этого же банка. Эту карту привезет курьер. Потерпевшая согласилась.

Она активировала в приложении уже имевшуюся кредитную карту на сумму 162 000 рублей. Далее она утратила контроль за приложением этого банка. Войти в него уже не получалось. Когда и как она передала пароли и коды от приложения, потерпевшая пояснить не может.

«Специалист службы безопасности Центробанка» лишь сообщил ей имя курьера и дату его приезда.

Новую карту с кредитным лимитом 187 000 рублей привезла из соседнего города курьер банка. Оформление документов по этой кредитной карте происходило под чутким руководством «специалиста службы безопасности Центробанка». По телефону он давал потерпевшей указания в процессе оформления этой карты. Видя, что потерпевшая действует самостоятельно, курьер банка никак на это не отреагировала.

Впоследствии денежные средства с этих кредитных карт были сняты неизвестными лицами. Потерпевшая сама деньги не снимала.

Далее злоумышленники попытались склонить потерпевшую к продаже ее квартиры. Однако квартира находилась в долевой собственности Светланы Х. и ее дочерей. Поэтому эта цель мошенниками не была реализована.

Таким образом, у потерпевшей образовалась задолженность в сумме 1 199 000 рублей.

Потерпевшая обратилась с заявлением в правоохранительные органы только после того, как о сложившейся ситуации узнали ее взрослые дочери и забили тревогу.

По заявлению потерпевшей возбуждено уголовное дело, однако преступники не установлены. Расследование дела периодически приостанавливается и возобновляется после жалоб потерпевшей в прокуратуру.

Следователь прямо говорит потерпевшей, что все это формально, и злоумышленники никогда не будут найдены и привлечены к ответственности.

Помимо того, что преступники остаются безнаказанными, возникает еще одна серьезная проблема. Банки обращаются в суд с исками о взыскании с потерпевшей задолженности по кредитам. Суды всех инстанций встают на сторону банков, мотивируя свое решение тем, что отсутствует приговор суда. Виновные не установлены, факт мошенничества не доказан. Будет приговор – взыскивайте с осужденных. А приговора нет и никогда не будет.

В рамках гражданского дела нами уже пройдены две судебные инстанции: первая и апелляционная. Обе инстанции встали на сторону банков.

В результате мошеннических действий у потерпевшей возникла задолженность более 1 250 000 рублей. Для нее это неподъемная сумма. Оплатить она ее не сможет. Потерпевшая пенсионерка и продолжает работать воспитателем в детском саду. Ее доход 30 000 в месяц (пенсия + заработная плата).

Случившееся стало для нее большим потрясением. Этот случай далеко не единичный. Дистанционное мошенничество превратилось в настоящую эпидемию.

В ходе опроса сотрудников правоохранительных органов, работающие над раскрытием и расследованием кибермошенничеств: оперуполномоченные отделов по борьбе с экономическими преступлениями и следователи следственных управлений, было выявлено, что данные преступления совершаются большими организованными группами. Структуру этих групп можно представить следующим образом:

1. Группа, занимающаяся сбором персональных данных о гражданах: покупка и хищение персональной информации (ФИО, сведения об имеющихся банковских картах, номера телефонов и т.д.).

2. Группа, занимающаяся подбором лиц – пособников совершения преступлений: дропперы, курьеры и т.д.

Дроппер – это человек, который за небольшое вознаграждение оформляет на себя пластиковую банковскую карту, на которую в дальнейшем будут поступать денежные средства потерпевших. После оформления карты дроппер оставляет карту в тайнике, координаты которого ему присылает куратор, и получает вознаграждение.

Из тайника карту забирает курьер, который либо в дальнейшем сам снимает с нее наличные и переводит деньги на реквизиты, указанные куратором, либо передает эту карту другому лицу. Курьер также получает вознаграждение.

Дроппер также может быть лицом, которое оформляет на свои паспортные данные карты IP – телефонии, которые затем по той же схеме передаются мошенникам.

По словам сотрудников правоохранительных органов, эти лица к уголовной ответственности не привлекаются. При их задержании они заявляют, что просто хотели подзаработать и отношения к мошенникам не имеют.

3. Лица, отвечающие за аренду номеров IP - телефонии. Аренда номеров осуществляется посредством интернет-сервисов. На этих сервисах мошенники регистрируются, предоставляя ресурсу свои реальные данные, оплачивают аренду номера. Аренда новых номеров производится мгновенно по мере возникновения необходимости в ходе психологической обработки потерпевшего.

4. Операторы. Это лица, непосредственно контактирующие с потерпевшим, осуществляющие обзвон и дальнейшую психологическую обработку потерпевшего.

Все злоумышленники проходят серьезное обучение и подготовку.

Один из следователей рассказал о потерпевшем, который, после звонка мошенников с сообщением, что его дочь попала в беду, перевел денежные средства в достаточно крупной сумме. А дочери у потерпевшего нет. После вопроса следователя, зачем тогда он перевел деньги. Потерпевший пояснил, что хотел помочь девушке, попавшей в беду, настолько убедительны были мошенники.

Полагаем, что это не исчерпывающий перечень категорий лиц, задействованных в мошеннических схемах.

Опрошенные сотрудники правоохранительных органов рассказали, что работа по психологической обработке потерпевшего идет по четкому алгоритму. Мошенники никогда не переходят к следующему этапу, не закрепив предыдущий.

Что касается мошенничеств с последующим хищением денежных средств (личных или кредитных) посредством сервисов онлайн-банкинга, обобщенно алгоритм можно представить следующим образом:

1. Звонок от «сотрудника банка» с вопросами или информацией:
 - подавали ли Вы заявку на смену номера телефона в приложении банка?
 - подавали ли Вы заявку на получение кредита?
 - Вам одобрен кредит в сумме...
 - с Вашей карты была осуществлена попытка перевода денег...
 - и т.п.

На этой стадии потерпевшему заявляют: «Не сообщайте сейчас номер карты, CVV - код и коды из смс. Информация конфиденциальная. Я переведу Вас на сотрудника «службу безопасности банка», усыпляя тем самым бдительность потерпевшего.

Сам факт перевода звонка также вызывает у потерпевшего доверие. Он убеждается в том, что это банк – большая серьезная организация. При разговоре потерпевший слышит фоновые шумы – безобидные рабочие разговоры других специалистов с клиентами.

2. Перевод звонка на «сотрудника службы безопасности банка» или на «сотрудника службы безопасности Центробанка». Лицо, выполняющее роль этого сотрудника владеет банковской терминологией, говорит убедительно и жестко. Объясняет, что такое защищенные ячейки (счета) Центробанка. Поместить деньги на эти счета – единственный способ спасения для потерпевшего.

3. Звонок высокопоставленного «сотрудника правоохранительных органов» с подменного номера, который определяется у потерпевшего как реальный номер этой правоохранительной структуры.

Потерпевший либо верит той информации, что автоматически определил его мобильный телефон. Либо проверяет номер на официальном сайте этого органа, убеждаясь в правильности номера телефона.

На этой стадии потерпевшего убеждают, что хотят помочь ему. С их помощью потерпевший сможет спасти себя, спасти свои деньги.

Убеждают в необходимости соблюдать конфиденциальность. Предлагают придумать кодовые слова, чтобы с их помощью распознавать, кто ему звонит – свой или чужой.

На электронную почту и в мессенджеры потерпевшего направляются сканы удостоверений, приказов и прочих документов, подтверждающих серьезность проводимых мероприятий.

Благодаря слаженным действиям потерпевшего и сотрудников спецслужб банда мошенников будет разоблачена и наказана.

4. Далее с потерпевшим связывается «сотрудник правоохранительных структур», который будет сопровождать потерпевшего во время «операции» (куратор). Он высылает потерпевшему сканы удостоверения с фотографией, сообщает немного информации о себе (возраст, наличие детей, стаж работы и т.д.).

Потерпевший убеждается в том, что ему будут постоянно помогать, подсказывать. Денежные средства будут спасены.

Потерпевшего убеждают в нечистоплотности сотрудников банка. Реальные сотрудники банков, отвечающие на звонки потерпевших в этот критический момент, играют на руку мошенникам, проявляя равнодушие, грубость и некомпетентность. А на горячие линии некоторых банков вообще невозможно дозвониться.

5. Куратор (оператор) постоянно находится на связи с потерпевшим. В любое время суток. Оперативно устраняет все сомнения потерпевшего, грамотно и убедительно отвечая на вопросы, высылая сканы документов.

В ходе общения с потерпевшим куратор выясняет дополнительные сведения – в каких еще банках есть счета и карты у потерпевшего, какая недвижимость находится в его собственности.

Если потерпевший очень внушаем, к «операции» добавляют и другие банки, совершают попытки оформить кредит с залогом имеющейся у потерпевшего недвижимости.

6. После того, как у потерпевшего похитили всё, что можно, куратор некоторое время поддерживает связь с ним. Убеждает в том, что мошенники вот – вот будут пойманы, присылает письма от банков о том, что у потерпевшего отсутствует задолженность перед банками.

Через какое-то время связь прекращается.

Обобщив собранную информацию можно сделать вывод о наличии серьезных проблем в сфере правового регулирования данного вида преступлений:

1. Отсутствие оперативного обмена информацией между правоохранительными органами и банками. Некоторые банки уже перешли на электронный документооборот (ЭДО) с правоохранительными структурами, где срок предоставления ответа на запрос составляет 3 суток. Однако это единицы. Большинство банков отвечает на запросы следователя целый месяц. В течение этого времени видеозаписи с банкоматов уничтожаются, утрачивается и иная необходимая следователю информация.

2. Пропуск операторами связи подменных номеров. Этот факт существенно облегчает мошенникам их деятельность и затрудняет правоохранительным органам раскрытие преступления. На установление реального номера телефона звонившего уходит очень много времени, а иногда это вообще невозможно.

22 декабря 2021 года Государственной Думой был принят Федеральный закон № 480-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», согласно которому устанавливается запрет на подмену номера при установлении голосовых соединений и передаче СМС — как в телефонной сети, так и в интернете. За неисполнение оператором связи передачи абонентского номера в неизменном виде должностные лица будут платить штраф в размере 30-80 тыс. рублей, ИП — 200-500 тыс. рублей, юридические лица — 500-800 тыс. рублей. Если оператор связи не прекратит оказание услуг связи или пропуск трафика в предусмотренных законодательством случаях, с должностного лица взыщут 50-100 тыс. рублей, с ИП — 400-800 тыс. рублей, с организации — 0,6-1 млн рублей. Штрафы в таком же размере будут взимать и с тех операторов связи, которые не подключатся к системе обеспечения соблюдения требования при оказании услуг связи и пропуска трафика в сети связи общего пользования [2]. Возможно, это поможет в предупреждении этой категории преступлений.

3. Наличие в интернете сервисов, сдающих в аренду номера телефонов. Большинство этих сервисов не сотрудничают с российскими правоохранительными структурами. Именно эти сервисы чаще всего владеют реальными данными злоумышленников.

4. Отсутствие специализированных отделов и групп в составе правоохранительных структур, обладающих специальными знаниями, необходимыми для раскрытия кибермошенничеств. Также правоохранительные органы остро нуждаются в сотрудниках, которые будут анализировать и систематизировать весь объем информации, поступающий в ходе расследования уголовного дела.

Некоторые авторы предлагают создавать специальные группы, состоящие из сотрудников подразделений уголовного розыска, отдела «К» БСТМ МВД России и представителей Роскомнадзора для проведения совместных проверок, в том числе с помощью мониторинга Интернет-ресурсов, направленных на выявление и документирование фактов нарушения законодательства в сфере связи, информационных технологий и массовых коммуникаций [1. С. 88-93].

5. Отсутствие заинтересованности банков в предупреждении и пресечении преступлений, связанных с оформлением кредитов. Судебная практика в настоящее время складывается в пользу банков. И банки знают, что в любом случае деньги будут взысканы с потерпевшего. А пострадавшему будет отказано в признании сделки недействительной даже в случае возбуждения уголовного дела и наличия у него статуса потерпевшего.

Если бы в таких случаях сделки аннулировались или хотя бы взыскание приостанавливалось до вынесения приговора мошенникам, а банк не получал бы возмещения, банки бы вели себя иначе. У них был бы стимул пресечь преступление на начальных этапах. Банк может оперативно выявить информацию о том, что изменился номер телефона, привязанный к приложению онлайн-банкинга, что вход в приложение осуществлен с нового IP – адреса и т.д.

6. Отсутствие строгих сроков хранения на банкоматах видеозаписей, которые сами по себе являются не только важной мерой профилактики возможных инцидентов (сдерживающим фактором), но и ценным источником оперативно-розыскной и криминалистической информации в процессе раскрытия и расследования преступлений [4. С. 243-248].

7. Отсутствие материальных ресурсов у правоохранительных структур для проведения активной разъяснительной работы в СМИ, для придания огласки вопиющим случаям кибермошенничества.

По словам опрошенных сотрудников правоохранительных органов, им даже приходится оплачивать из личных средств съемку и публикацию в СМИ видеороликов с разъяснительной информацией для населения.

Список литературы

1. Абышов Д. З., Потапова Н. Н. Некоторые особенности выявления и раскрытия бесконтактного мошенничества // Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 88-93.

2. Госдума запретила подменять номера при звонках и передаче СМС // <https://dumatv.ru/news/gosduma-zapretila-podmenyat-nomera-pri-zvonkah-i-peredache-sms>

3. Иванцов С. В., Молчанова Т. В. Информационно-телекоммуникационные технологии – современная реальность преступности // Вестник Санкт-Петербургского университета МВД России. 2020. № 4 (88). С. 89–96.

4. Любан В. Г. Проблемные аспекты банковской деятельности и деятельности операторов сотовой связи в борьбе с преступлениями в сфере информационных технологий // Вестник экономической безопасности. 2018. № 1. С. 243-248.

5. Озеров К. И. Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2021. № 1 (89). С. 167–171.

6. Озеров К. И., Озеров И. Н. Проблемы предупреждения мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий // Проблемы правоохранительной деятельности. 2021. № 1. С. 30 –34.

7. Озеров И. Н., Озеров К. И. Новые способы совершения мошеннических действий в сфере IT-технологий в период коронавирусной инфекции // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2021. № 1. С. 24–28.

8. <https://rg.ru/2020/06/09/medvedev-rasskazal-o-roste-kiberprestupnosti-v-rf-na-85-za-5-mesiacev.html> (дата обращения: 11.09.2022).

Ю. С. Гокунь,
магистрант,

Донецкий национальный университет

СОЗДАНИЕ ЕДИНОГО РЕГИСТРА СУРРОГАТНЫХ МАТЕРЕЙ И ДОНОРОВ БИОМАТЕРИАЛОВ И ОБЕСПЕЧЕНИЕ ЕГО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Целью исследования является обоснование необходимости создания Единого регистра суррогатных матерей и доноров биоматериалов и обеспечение его информационной безопасности. Определено, что принятие Федерального закона «О вспомогательных репродуктивных технологиях» является необходимой мерой, направленной на совершенствование российского правового поля. Установлено, что создание Единого регистра суррогатных матерей и доноров биоматериала упростит процесс поиска суррогатной матери тысячам лиц, обращающихся к вспомогательным репродуктивным технологиям. Обозначено, что в целях защиты конфиденциальных данных лиц, участвующих в программах в сфере вспомогательных репродуктивных технологий, особое внимание должно уделяться информационной безопасности Единого регистра суррогатных матерей и доноров биоматериала.

Ключевые слова: Единый регистр суррогатных матерей и доноров биоматериалов, база данных, конфиденциальность, медицинская тайна, личная тайна, семейная тайна, информационная безопасность

CREATION OF A UNIFIED REGISTER OF SURROGATE MOTHERS AND DONORS OF BIOMATERIALS AND ENSURING ITS INFORMATION SECURITY

Abstract. The purpose of the study is to substantiate the need to create a Unified register of surrogate mothers and biomaterial donors and ensure its information security. It has been determined that the adoption of the Federal Law “On Assisted Reproductive Technologies” is a necessary measure aimed at fulfilling the Russian legal framework. It has been established that the creation of the Unified register of surrogate mothers and biomaterial donors will simplify the process of searching for a surrogate mother for thousands of people applying for assisted reproductive technologies. It is indicated that in order to protect the confidential data of persons participating in programs in the field of assisted reproductive technologies, special attention should be paid to the information security of the Unified register of surrogate mothers and biomaterial donors.

Keywords: Unified register of surrogate mothers and donors of biomaterials, Database, Confidentiality, Medical secret, Personal secret, Family secret, Information security

Одним из самых актуальных вопросов здравоохранения на протяжении последнего десятилетия признается бесплодие. Стремительно усугубляющееся ухудшение состояния окружающей среды, ведение нездорового образа жизни [4. С. 43–46], гормональные нарушения, физические и психические травмы, стрессы, врожденные аномалии и генетические патологии крайне негативно влияют на репродуктивное здоровье как мужчин, так и женщин, и зачастую становятся одними из наиболее распространенных причин бесплодия. По оценкам экспертов из Всемирной организации здравоохранения, во всем мире от 48 млн пар до 186 млн чел. страдают бесплодием [6]. Американский колледж акушерства и гинекологии, центры по контролю заболеваемости и Американское общество репродуктивной медицины предоставляют следующие данные:

- 1) лишь 25 % здоровых женщин, находящимся в возрасте от 20 до 30 лет, удается забеременеть в течение одного менструального цикла;
- 2) только 10 % женщин в возрасте 40 лет удается забеременеть в течение одного менструального цикла;
- 3) уже с 20–30 лет женская фертильность начинает снижаться, а после 35 лет она снижается значительно быстрее;
- 4) пары, в которых мужчина старше 40 лет, чаще испытывают сложности с зачатием [3].

Согласно отечественной статистике, каждая шестая семья в Российской Федерации сталкивается с проблемами, вызванными бесплодием [5], в результате которых супруги не могут стать родителями. Реализовать право на семью и помочь завести ребенка помогают вспомогательные репродуктивные технологии. Вспомогательные репродуктивные технологии принято рассматривать как наиболее эффективные методы лечения бесплодия, во время обращения к которым определенные этапы либо же каждый этап зачатия и раннего развития эмбрионов

проводятся вне материнского организма, включая сопровождаемые применением донорских и (или) криоконсервированных половых клеток, тканей репродуктивных органов и эмбрионов, а также суррогатного материнства [2].

Однако, несмотря на всю полезность вспомогательных репродуктивных технологий, их применение вызывает множество дискуссионных вопросов с точки зрения права. Во многом это обусловлено ненадлежащим нормативно-правовым регулированием данных методов лечения бесплодия, в частности, отсутствием специального Федерального закона «О вспомогательных репродуктивных технологиях», который бы сконцентрировал внимание не просто на технике и особенностях процесса осуществления вспомогательных репродуктивных технологий и сопутствующих им моментов, но и создал бы их подробное юридическое сопровождение. В Федеральном законе «О вспомогательных репродуктивных технологиях» должно быть предусмотрено наличие норм о создании и функционировании электронного регистра женщин, которые хотели бы стать суррогатными матерями, а также лиц, желающих стать донорами ооцитов и спермы. Предлагаемый нами регистр мог бы называться «Единый регистр суррогатных матерей и доноров биоматериалов».

Отметим, что в настоящий момент существует Регистр вспомогательных репродуктивных технологий, созданный Российской ассоциацией репродукции человека. Данный Регистр содержит в себе перечень репродуктивных клиник, центров и отделений, на основании сведений о деятельности которых Российская ассоциация репродукции человека формирует ежегодные отчеты. В указанном Регистре отсутствуют какие-либо данные о женщинах, которые бы хотели предоставить свои услуги по вынашиванию и рождению детей, а также о тех, кто хотел бы стать донорами биологического материала.

Единый регистр суррогатных матерей и доноров биоматериалов необходим, поскольку генетическим родителям, неспособным по медицинским показаниям иметь детей, в некоторых случаях бывает сложно найти женщину, которая хотела бы стать суррогатной матерью. Возникающие сложности обусловлены рядом причин, среди которых возможно выделить три основные, т. е. отсутствие либо нежелание родственниц и знакомых вынашивать и рожать чужого ребенка, отсутствие потенциальных кандидаток на роль суррогатной матери, а также желание генетических родителей сохранить конфиденциальность и скрыть истинный способ появления ребенка на свет. Намерение генетических родителей скрыть настоящий способ появления ребенка подталкивает их на сотрудничество с репродуктивными клиниками, находящимися в соседних городах либо даже в других областях и краях Российской Федерации. Кроме того, некоторые родители предпочитают в качестве суррогатной матери выбирать именно ту женщину, у которой ранее уже был подобный и, что самое главное, благополучный опыт. В свою очередь, аналогичную полностью достоверную информацию они могли бы получить из Единого регистра суррогатных матерей и доноров биоматериалов при обращении в репродуктивную клинику.

В Едином регистре суррогатных матерей и доноров биоматериалов должна быть отражена информация о женщинах, подходящих для становления суррогатной матерью по следующим критериям: возраст, надлежащее физическое и психическое

здоровье, отсутствие медицинских противопоказаний, наличие хотя бы одного здорового ребенка, отсутствие хирургических вмешательств на репродуктивных органах и проводимого кесарева сечения, протекание предыдущих беременностей и родов без осложнений. В предлагаемом нами регистре применительно к донорам спермы и ооцитов должны содержаться сведения следующего типа: о надлежащем физическом и психическом здоровье, о том, что они не состоят на учете в психоневрологическом и наркологическом диспансере, о группе крови и резус-факторе, о фенотипических признаках, т. е. цвет глаз, волос, рост, вес и т. д.

Единый регистр суррогатных матерей и доноров биоматериалов должен быть подконтролен Министерству здравоохранения Российской Федерации. Изменения в него могут вноситься репродуктивными клиниками, центрами и отделениями.

Обратим внимание на то, что в целях обеспечения конфиденциальности, охраны медицинской, семейной и личной тайны особое внимание должно уделяться информационной безопасности электронного Единого регистра суррогатных матерей и доноров биоматериалов. Активно происходящая цифровизация несет новые угрозы, главными из которых признаются взлом и утечка конфиденциальных данных. С развитием информационно-телекоммуникационных технологий угроза раскрытия личной информации становится все более реальной. Ежегодно появляются новые виды вредоносных программ (вирусы, компьютерные черви, трояны, руткит, бэкдор и др.), способных получить несанкционированный доступ к закрытой информации, модифицировать, завладеть и стереть ее. Так, такое вредоносное программное обеспечение, как бэкдор, представляющее собой средство удаленного администрирования, предоставляет третьему лицу возможность управлять компьютером удаленно. Различные виды бэкдора позволяют хакерам устанавливать и запускать на чужом компьютере любое программное обеспечение, фиксировать последовательность нажатия клавиш, загружать, скачивать и сохранять любые файлы, изучать сведения, хранящиеся на устройстве, включать камеру либо микрофон, получая таким образом абсолютный контроль над компьютером и чужой личной информацией. При этом, жертвой может стать как индивидуальное физическое лицо, так и какой-либо сотрудник субъекта хозяйствования. Второй вариант подразумевает причинение значительного ущерба всему предприятию либо фирме, а не только какому-то конкретному сотруднику. Следовательно, ни одна организация не застрахована от возможной утечки данных [6. С. 100–108].

Отметим, что в случае утечки данных из Единого регистра суррогатных матерей и доноров вред будет причинен сразу нескольким участникам рассматриваемых правоотношений, а именно физическим лицам (потенциальным суррогатным матерям и донорам, а возможно и генетическим родителям в том случае, если из-за утечки конфиденциальных данных потенциальная суррогатная мать откажется участвовать в программе), репродуктивным клиникам, центрам и отделением, а также Министерству здравоохранения Российской Федерации как контролирующему и ответственному за ведение Регистра субъекту. При наступлении описанной ситуации репродуктивной клинике и Министерству здравоохранения Российской Федерации ущерб будет причинен, главным образом, их репутации и, возможно, одним из негативных последствий станет снижение доверия отече-

ственным репродуктивным клиникам со стороны пациентов, а значит и снижение количества случаев обращения к вспомогательным репродуктивным технологиям, что в свою очередь, вполне способно ухудшить демографическую ситуацию в Российской Федерации.

На наш взгляд, особый ущерб причинит завладение, раскрытие и разглашение информации об обращении лица к вспомогательным репродуктивным технологиям. Следствием этого станет причинение моральных травм итак расстроенному человеку из-за проблем со здоровьем и отсутствием возможности завести ребенка естественным путем.

Полагаем, уязвимость жертвы хакерской атаки обусловлена двумя факторами, т. е. недостаточным уровнем информационной безопасности субъекта хозяйствования, осуществляющего деятельность в сфере здравоохранения, и более продвинутым уровнем пользования информационно-телекоммуникационными технологиями хакера. В дополнение к этому, ни в одном нормативно-правовом акте не регламентирован вопрос обеспечения информационной информации баз данных, которой по своей сущности и является Единый регистр суррогатных матерей и доноров биоматериалов. В связи с этим, предлагаем сделать первый шаг в данном направлении и закрепить в Федеральном законе «О вспомогательных репродуктивных технологиях» положения об информационной безопасности Единого регистра суррогатных матерей и доноров биоматериалов, касающиеся:

- 1) общих принципов управления безопасностью Регистра;
- 2) задач по обеспечению информационной безопасности Регистра;
- 3) механизма обеспечения информационной безопасности Регистра.

Таким образом, вышеуказанные законодательные новеллы предлагаем изложить в следующей редакции:

Глава Единый регистр суррогатных матерей и доноров биоматериалов

Статья Единый регистр суррогатных матерей и доноров биоматериалов как база данных

1. Единый регистр суррогатных матерей и доноров биоматериалов представляет собой базу данных, содержащую сводную информацию из репродуктивных клиник, центров и отделений о женщинах, желающих принять стать суррогатными матерями, и о лицах, желающих предоставить свои ооциты и сперму в качестве донорских.

2. Полномочным органом по контролю за Единым регистром суррогатных матерей и доноров биоматериалов является Министерство здравоохранения Российской Федерации.

Статья Обеспечение информационной безопасности Единого регистра суррогатных матерей и доноров биоматериалов

1. К общим принципам управления безопасности Единого регистра суррогатных матерей и доноров биоматериалов относятся:

1) использование защищенного сервера либо платформы Единого регистра суррогатных матерей и доноров биоматериалов, имеющего собственные системы аудита и мониторинга;

2) ограничение физического доступа к компьютерам, на которых находятся элементы Единого регистра суррогатных матерей и доноров биоматериалов;

3) обеспечение наличия системы резервного копирования и восстановления Единого регистра суррогатных матерей и доноров биоматериалов после сбоев;

4) исключение возможности запуска любых программ либо процессов на сервере с Единым регистром суррогатных матерей и доноров биоматериалов.

2. Функционирование Единого регистра суррогатных матерей и доноров биоматериалов осуществляется за счет выполнения следующих задач по обеспечению информационной безопасности Регистра:

1) защита информации от несанкционированного доступа третьих лиц;

2) предотвращение уничтожения данных;

3) защита от программных и аппаратных ошибок и сложностей с доступом к серверу, затрудняющих либо полностью препятствующих обработке информации, которая содержится в Едином регистре суррогатных матерей и доноров биоматериалов.

Подытожив все вышеизложенное, считаем целесообразным обозначить основные выводы, полученные в результате проведенного исследования:

1) принятие Федерального закона «О вспомогательных репродуктивных технологиях» является необходимой мерой, направленной на совершение российского правового поля;

2) создание Единого регистра суррогатных матерей и доноров биоматериала упростит процесс поиска суррогатной матери тысячам лиц, обращающихся к вспомогательным репродуктивным технологиям;

3) в целях защиты конфиденциальных данных лиц, участвующих в программах в сфере вспомогательных репродуктивных технологий, особое внимание должно уделяться информационной безопасности Единого регистра суррогатных матерей и доноров биоматериала.

Список литературы

1. Бесплодие в России в мире // Репробанк. Банк репродуктивных тканей. URL: <https://reprobank.ru/novosti/stati/besplodie-v-rossii> (дата обращения: 08.08.2022).

2. Иванова А. П. Утечка персональных данных: большая проблема в цифровую эпоху // Реферативный журнал. 2020. № 4. С. 100–108.

3. Каждая шестая супружеская пара имеет проблемы с деторождением // MR RU. URL: <https://www.mk.ru/social/health/2022/08/02/kazhdaya-shestaya-supruzheskaya-para-imeet-problemy-s-detorozhdeniem.html> (дата обращения: 08.08.2022).

4. Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон от 21.11.2011 № 323-ФЗ// СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 09.08.2022).

5. Очирова Э. С. О понятии суррогатного материнства в законодательстве Российской Федерации // Вестник науки и образования. 2020. № 14–1 (92). С. 43–46.

6. Infertility // World Health Organization. URL: <https://www.who.int/news-room/fact-sheets/detail/infertility> (дата обращения: 08.08.2022).

И. В. Горячев,

доцент,

Ивановский филиал Российской академии народного
хозяйства и государственной службы
при Президенте Российской Федерации

О ЦИФРОВЫХ ТЕХНОЛОГИЯХ УПРАВЛЕНИЯ КАДРОВЫМ СОСТАВОМ ГОСУДАРСТВЕННОЙ СЛУЖБЫ В СОВРЕМЕННЫХ ИССЛЕДОВАНИЯХ

Аннотация. В условиях развития цифровизации государственного управления происходит более широкое применение информационно-коммуникационных технологий как в управленческой деятельности органов государственной власти, так и в управлении кадровыми процессами на государственной службе. Различные аспекты реализации цифровых кадровых технологий в органах государственной власти неизменно находятся в поле зрения современных исследователей. Проанализирован поток публикаций по использованию цифровых кадровых технологий на государственной службе. В целом количество публикаций по данной теме возрастает, хотя исследований обобщающего характера (диссертаций, монографий) относительно немного. Выявлены характерные черты и основные направления публикационной активности исследователей.

Ключевые слова: цифровые технологии, кадровый состав, государственная служба, государственное управление, информационно-коммуникационные технологии, правовое обеспечение цифровых кадровых технологий, органы государственной власти

ABOUT DIGITAL TECHNOLOGIES FOR MANAGING THE STAFF OF THE PUBLIC SERVICE IN MODERN RESEARCH

Annotation. The flow of publications on the use of digital HR technologies in the public service is analyzed. In general, the number of publications on this topic is increasing, although there are relatively few studies of a generalizing nature (dissertations, monographs). The characteristic features and main directions of researchers' publication activity are revealed.

Keywords: Digital technologies, Staffing, Civil service, Public administration, Information and communication technologies, Legal support of digital personnel technologies, Public authorities

Современные социально-экономические, культурные процессы, протекающие в российском обществе, развитие сферы информационно-коммуникационных технологий оказывают существенное влияние на сферу государственного управления, обуславливают ее трансформацию, актуализируют необходимость совершенствования управленческой деятельности органов государственной исполнительной власти, повышения качества оказания государственных услуг населению и организациям.

Важным ресурсом для повышения эффективности управленческой деятельности органов государственной исполнительной власти является кадровый состав органов государственной исполнительной власти. Для всестороннего раскрытия и использования кадрового потенциала органов власти используются кадровые технологии. Их основными направлениями реализации являются:

- профессиональная адаптация, ориентация, мотивация и оценка кадров;
- применение антикоррупционных технологий;
- информатизация и автоматизация кадровых процессов в органах государственной исполнительной власти и др. [4]

В связи с важностью применения современных кадровых технологий в сфере государственного управления Министерством труда и социальной защиты на протяжении ряда лет проводится конкурс, целью которого являются выявление и масштабирование лучших кадровых практик в системе государственного управления, в том числе по направлению применения кадровых цифровых и информационно-коммуникационных технологий [4].

Несомненно, что применение кадровых технологий в сфере управления кадровым составом государственной службы оказывает существенное влияние на количественные и качественные характеристики контингента государственных служащих [3. С. 285–288].

В настоящее время отдельные правовые, организационно-правовые и другие аспекты реализации кадровых цифровых технологий на государственной гражданской службе находятся в поле пристального внимания исследователей. Наблюдается увеличение потока публикаций на интересующую нас тему. Согласно данным, предоставленным РИНЦ по запросу «цифровые кадровые технологии» (без учета совпадений), было выявлено 834 публикации по вопросам применения данных технологий. По имеющимся в нашем распоряжении данным, прирост публикаций в период 2018–2021 гг. составил 23 %.

Распределение указанных 834 публикаций по темам представлено в следующей таблице.

Тематика публикаций по вопросам применения цифровых технологий управления кадровым составом государственной службы и распределение в %

Тематическое направление публикаций	Количество публикаций, %
Правовое обеспечение реализации цифровых и информационно-коммуникационных технологий на государственной службе	20
Опыт (оценка) применения цифровых кадровых технологий на примере конкретных органов государственной власти	10
Опыт (оценка) применения цифровых кадровых технологий на примере субъектов РФ	25
Реализация цифровых кадровых технологий по функциям кадрового менеджмента	25
Проблемные аспекты использования кадровых и информационно-коммуникационных технологий в управлении кадровым составом государственной службы	10
Прочая тематика	10

Следует обратить внимание на комплекс публикаций в научных периодических изданиях, в которых авторами специально или попутно рассматриваются следующие вопросы:

- перспективы внедрения цифровых технологий в служебную деятельность органов государственной власти, их территориальных и структурных подразделений (в том числе кадровых) [2. С. 1136–1142];
- значение цифровых технологий для системы государственного управления и формирования кадрового состава органов власти;
- применение цифровых кадровых технологий на государственной службе в контексте цифровизации государственного управления;
- развитие цифровых компетенций государственных гражданских служащих [1. С. 28–42; 6. С. 43–49].

В рамках проводимых научных мероприятий (научных, научно-практических конференций, круглых столов и др.), посвященных исследованию перспективных аспектов современного государственного управления, исследователями обсуждаются вопросы применения цифровых кадровых технологий на государственной службе, что находит свое отражение в опубликованных материалах сборников научных, научно-практических и прочих конференций. Среди наиболее часто рассматриваемых аспектов применения цифровых кадровых технологий на государственной службе следует выделить:

- прикладные цифровые технологии в процессах взаимодействия органов власти и граждан;
- вопросы цифровизации профессионального развития кадрового состава органов власти;
- использование цифровых технологий для оптимизации управления кадровым составом государственной службы и др. [5. С. 369–374]

Применение кадровых технологий на государственной гражданской службе в цифровом формате происходит в соответствии с нормами действующего законодательства. Особенности организации их применения с точки зрения правового обеспечения заключаются в следующем:

- инициирование проектирования кадровых технологий и их последующее внедрение происходит как во исполнение действующих нормативных правовых актов Президента Российской Федерации и Правительства Российской Федерации по вопросам государственной службы, так и властями субъектов РФ по собственной инициативе;
- реализация кадровых технологий на государственной гражданской службе осуществляется на правовой основе, имеющей во многом как организационно-правовой, так и нормативно-методический характер. Как правило, в положениях о внедрении в практическую работу органов государственной власти цифровых технологий конкретизируются цели и задачи создания той или иной цифровой системы, определяется порядок ее функционирования, фиксируются ее функциональные подсистемы, определен порядок доступа пользователей, работающих с цифровой системой и др.;
- достаточно часто правовые акты органов государственной исполнительной власти по вопросам использования кадровых цифровых технологий на госу-

дарственной службе дополняются материалами методического характера. К ним, в частности, относятся регламенты по работе с информационными системами по кадровому составу органов государственной исполнительной власти регионов и др.

Подводя итог вышесказанному, следует отметить, что в настоящее время наблюдается значительный интерес со стороны исследователей к вопросам применения цифровых технологий на государственной службе, прослеживается отчетливая тенденция к увеличению количества публикаций по данной теме. В структуре потока публикаций основную долю занимают статьи в периодических научных изданиях, а также публикации в сборниках научных, научно-практических конференций, материалов круглых столов и т. д. При этом доля диссертаций и монографий по вопросам использования цифровых кадровых и информационно-коммуникационных технологий в общем потоке научно-исследовательских работ относительно невелика. Это может быть связано с продолжающимся процессом развития нормативно-правовой базы реализации информационно-коммуникационных технологий на государственной службе, с накоплением исследователями репрезентативных эмпирических и других данных, необходимых для проведения более углубленных изысканий обобщенного характера.

Список литературы

1. Васильева Е. В., Пуляева В. Н., Юдина В. А. Развитие цифровых компетенций государственных гражданских служащих Российской Федерации // Бизнес-информатика. 2018. № 4 (46). С. 28–42.
2. Жиляев В. В. Перспективы внедрения цифровых технологий в служебную деятельность кадровых подразделений учреждений и органов уголовно-исполнительной системы // Инновации. Наука. Образование. 2021. № 27. С. 1136–1142.
3. Кропотова О. А., Горячев И. В. О динамике численности и гендерной структуре работников, замещающих должности государственной гражданской службы субъектов Российской Федерации (на материалах Федеральной службы государственной статистики) // Равноправие мужчин и женщин в России и в мире: научный потенциал молодежных исследований: материалы Международной молодежной науч. конф. Иваново, 19 марта 2022 г. Иваново: Ивановский государственный университет, 2022. С. 285–288.
4. Министерство труда и социальной защиты Российской Федерации: официальный сайт. URL: <https://mintrud.gov.ru/ministry/programms/gossluzhba/17/17> (дата обращения: 15.09.2022).
5. Пыжова Н. Н. Потребности кадровых служб государственных органов и организаций в использовании цифровых технологий для оптимизации HR-процессов // Психология управления персоналом и экосистемами наставничества в условиях изменения технологического уклада: материалы Второй международной науч.-практ. конф. Нижний Новгород, 12–13 ноября 2021. Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н. И. Лобачевского, 2021. С. 369–374.
6. Щехочихина С. В., Рыжакова Е. В., Хазми А. Цифровые технологии в определении перспективного облика государственной службы // Муниципальная академия. 2019. № 1. С. 43–49.

А. И. Гретченко,

доктор экономических наук, профессор,
Российский экономический университет имени Г. В. Плеханова;
Финансовый университет при Правительстве Российской Федерации

А. А. Гретченко,

кандидат экономических наук, доцент,
Российский экономический университет имени Г. В. Плеханова

ОЦЕНКА УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ТРУДОВЫХ ПРОЦЕССОВ

Аннотация. Четвертая промышленная революция (Индустрия 4.0) – инициатива, основанная на цифровизации и ориентированная на появление новых интеллектуальных знаний. Индустрия 4.0 меняет то, как устроен мир. Цифровизация, один из столпов индустрии 4.0, оказывающая влияние на человеческий капитал и рынок труда. С одной стороны, некоторые рабочие места теряются, а с другой стороны, возникают новые рабочие места. Предприятиям потребуется высококвалифицированный персонал, чтобы оставаться конкурентоспособными на рынке. В статье рассматриваются не существовавшие ранее вызовы и угрозы информационной безопасности, которые имеют отношение к цифровизации экономики, способны оказывать влияние на самостоятельность бизнеса, а также на способность предприятий конкурировать, и в целом несут угрозу безопасности государства в сфере информации.

Ключевые слова: Четвертая промышленная революция (Индустрия 4.0), цифровизация, информационная безопасность, система национальной безопасности, цифровые технологии, кибератаки, информационно-телекоммуникативные сети

INDUSTRY 4.0 AND ASSESSMENT OF THE LEVEL OF INFORMATION SECURITY IN RUSSIA IN THE CONTEXT OF DIGITALIZATION OF LABOR PROCESSES

Abstract. The Fourth Industrial Revolution (Industry 4.0) is an initiative based on digitalization and focused on the emergence of new intellectual knowledge. Industry 4.0 is changing the way the world works. Digitalization, one of the pillars of industry 4.0, has an impact on human capital and the labor market. On the one hand, some jobs are being lost, and on the other hand, new jobs are being created. Enterprises will need highly qualified personnel to remain competitive in the market. The article examines previously non-existent challenges and threats to information security that are related to the digitalization of the economy, are able to influence the independence of business, as well as the ability of enterprises to compete, and in general pose a threat to the security of the state in the field of information.

Keywords: the Fourth Industrial Revolution (Industry 4.0), Digitalization, information security, National security system, Digital technologies, Cyber attacks, information and telecommunication networks

Введение. Индустрия 4.0 представляет собой четвертую промышленную революцию, сочетающую современные технологии с человеческим капиталом (сотрудники, менеджеры, студенты, преподаватели и т. д.). Следует отметить, что человеческий капитал включает в себя все знания, навыки, компетенции, способности, с которыми человек рождается, но также и те, которые человек приобретает в течение своей жизни, например, путем обучения, взаимодействия с другими людьми или получения работы.

Цифровые технологии все чаще становятся частью жизни людей – в личной и профессиональной жизни. Взаимосвязь современных технологий с человеческим капиталом также была продемонстрирована в COVID-19, когда сотрудники начали работать из дома (насколько позволяет характер их работы). В это время как российским, так и зарубежным компаниям приходилось приспосабливаться к сложившейся ситуации. Они также использовали цифровые технологии непосредственно для набора новых сотрудников – вместо личного собеседования они перешли на цифровой подбор персонала через различные онлайн-платформы (MS Teams, Zoom, Google Meets и др.).

Индустрия 4.0 основана на цифровизации и ориентирована на появление новых интеллектуальных фабрик. Четвертая промышленная революция основана на концепции интеллектуальных знаний, которые характеризуются тремя факторами, а именно быстрыми экспоненциальными темпами развития, появлением беспрецедентных парадигм в экономике, бизнесе, обществе и, наконец, внутренней трансформацией всех систем.

Этот тип промышленной революции очень сильно изменяет то, как люди живут, работают и общаются. Происходит постепенное перемещение отдельных сфер жизни людей из текущей (физической) в цифровую среду. Важно отметить, что человек больше не обладает полной властью и контролем над этой средой, поскольку она контролируется различными алгоритмическими правилами.

Индустрия 4.0 – это еще одна форма цифровизации и интеграции информационно-коммуникационных технологий (ИКТ). Основные элементы индустрии 4.0 включают анализ больших данных, автономных роботов, моделирование, горизонтальную и вертикальную системную интеграцию, Интернет вещей, 3D-печать, аддитивное производство, облачные системы, киберзащиту данных, обеспечивая информационную безопасность.

Цифровизация считается элементом индустрии 4.0, но вопрос в том, какое влияние ожидается от этого элемента на роль и положение человеческого капитала в будущем, и обеспечение его безопасности до настоящего времени остается открытым. Человеческий капитал считается врожденными и приобретенными навыками, знаниями, способностями, которыми владеет индивид.

Человеческий капитал в настоящее время становится центральным источником развития бизнеса и экономики в целом. Во времена цифровизации экономики это считается одним из инструментов конкурентной политики. Однако это не физический актив, а нематериальный капитал сотрудников.

Человеческий капитал в современном мире является основой, которая развивает конкурентоспособность компаний и позволяет им получать определенные

конкурентные преимущества. Цифровизация требует высококвалифицированного персонала, обладающего необходимыми знаниями и навыками в области информационных технологий/ИКТ и цифровых технологий. Только в этом случае это принесет добавленную стоимость не только для компании, но и для самой национальной экономики страны. Характер работы также изменится, обычная рутинная деятельность будет выполняться машинами и оборудованием (современные ИС/ ИКТ). По этой причине сотрудникам придется повышать уровень своего образования, систематически повышать свою квалификацию и проходить переподготовку.

Цифровые навыки – это наиболее актуальная группа способностей, навыков и знаний людей, относящихся к индустрии 4.0. Благодаря им сотрудники могут использовать цифровые технологии (ИС/ИКТ) так, чтобы они их понимали. Работа с компьютерами и другими ИС/ИКТ (поиск, обработка, хранение и представление данных) стала проще, чем раньше. Если кто-то хочет развить свои навыки, он должен сосредоточиться на пяти областях: информационная грамотность, коммуникация и сотрудничество, создание цифрового контента, безопасность, решение проблем.

Методология и методы исследования. Исследовательская работа в контексте данной темы проводилась на базе НИИ «Новая экономика и бизнес» Российского экономического университета имени Г. В. Плеханова. Информационная база была сформирована на основе ключевых слов. Введя ключевые слова «цифровизация, человеческий капитал», «информационная безопасность» в известную базу данных Web of Science вместе с ограничением по годам (2016–2021), было отображено только в России 82 статьи, из которых только 56 имели доступ к «открытому доступу». В ходе анализа научной литературы было выявлено, что у российских авторов разные взгляды на этот вопрос. Однако общий вывод: отечественные компании знакомы с термином «Индустрия 4.0», они воспринимают его в отношении человеческого капитала и рынка труда. Предполагается, что существует разница во внедрении цифровизации в бизнес-процессы с точки зрения размера компании, типа компании или отрасли, в которой она работает.

При проведении исследований, касающихся практики влияния цифровизации как одного из элементов Индустрии 4.0 на положение человеческого капитала и обеспечение его информационной безопасности, авторы статьи использовали следующие методы: метод описания, метод анализа, историко-генетический метод, корреляционный анализ, регрессионный анализ, метод мета-анализа данных. Для выводов, основанных на анализе литературы, был использован междисциплинарный исследовательский подход.

Результаты и обсуждения. Проанализированное авторское исследование полученных результатов указывает на преимущества, которые российские компании и организации получают от внедрения цифровизации, в основном горизонтальных и вертикальных (внутренних процессов) цепочек или цифровых продуктов. Важность подготовки компаний к цифровизации также подтверждается тем фактом, что цифровые доходы компании могут увеличиваться на 2,9 % в год. Как показывает практика, благодаря современным и цифровым технологиям отечественные компании могут сократить сроки доставки, повысить качество своих продуктов и услуг и, наконец, сэкономить деньги (экономия затрат).

Исследование проводилось на основе опроса в девяти доминирующих отраслях промышленности (промышленное производство; строительство; химическая промышленность; электротехника; транспорт и логистика; автомобильная промышленность; металлургия; другие отрасли промышленности; деревообрабатывающая и бумажная промышленность; авиация, аэрокосмическая промышленность, оборона и безопасность).

Это исследование также указывает на то, что в рамках Индустрии 4.0 проблема для отечественных компаний заключается не в современных технологиях, а в людях, рабочей силе, человеческом капитале. Это связано с тем, что успех бизнеса гарантируют не современные технологии, которые закупает компания, а работники, обладающие цифровым интеллектом. В то же время, в ходе опроса выяснилось, что до 38 % респондентов удовлетворены средними специальными навыками своих сотрудников. Очень важно, чтобы компания приобретала и располагала квалифицированной рабочей силой в данной области. Повышение уровня цифровых технологий в компании при одновременном повышении квалификации и квалификации сотрудников до 69 % компаний считают наиболее актуальной задачей в Индустрии 4.0.

Данные опроса показывают, что проблема также возникает из-за отсутствия видения и управленческой поддержки (40 %), неясных и плохо определенных экономических выгод от внедрения элементов индустрии 4.0 на практике (38 %), а также из-за нехватки средств (36 %). Несмотря на эту проблему, до 50 % компаний считают, что на процесс принятия решений в компании все больше влияют инструменты обработки данных и создания различных аналитик.

В связи с индустрией 4.0 также обсуждается безопасность корпоративных данных. В рамках этой группы рисков до 54 % респондентов опасаются кибератак, которые прервут работу компании на определенный период. Проблемы также включают сложное определение ответственности за потерю и повреждение данных компании (40 %), несанкционированное изменение и манипулирование данными компании внутри компании (40 %) или ущерб деловой репутации компании из-за потери конфиденциальных данных (39 %).

Как уже отмечалось ранее, цифровая революция (Индустрия 4.0) оказывает влияние на человеческий капитал. Именно благодаря людям и их знаниям, навыкам и способностям предприятия могут лучше использовать технологии. Если компании, а также сотрудники увидят положительное влияние технологий на человеческий капитал, это также повлияет на эффективность их работы и мотивацию. Поэтому основное внимание в исследовании уделялось влиянию цифровых технологий на управление человеческим капиталом.

Аналогичные исследования проводились отдельными группами российских ученых-экономистов. Так, исследование проф. Е. А. Федоровой фокусируется на восприятии цифровизации управления человеческим капиталом с точки зрения корпоративных сотрудников. Было выяснено, как современные технологии, которые приносит с собой Индустрия 4.0, повлияли на жизнь сотрудников, а также боятся ли они, что из-за них потеряют работу [13. С. 740–749].

В исследовании использовался нарративный анализ, который относится к методам качественного исследования. Обратившиеся сотрудники записали свои мысли

на бумаге. Тема «Опишите, как информационно-коммуникационные цифровые технологии повлияли на вашу работу и как их внедрение в компании может повлиять на ваше будущее» [13. С. 740–749]. В ходе этих интервью авторы получили необходимые данные, которые они в дальнейшем проанализировали, обработали и интерпретировали. В интервью приняли участие 57 респондентов (35 женщин и 22 мужчины) в возрастной категории 22–41 год, которые работают в различных отраслях экономики. Уровень использования цифровых технологий в компаниях варьируется. Одна компания может внедрить технологию, но другая не хочет ее использовать и переходит к другой. В России был проведен опрос, в котором в 2017 г. приняли участие до 159 компаний, которые были разделены на 13 групп по секторам «розничная торговля, производство, банковское дело и финансы, ИТ, транспорт, энергетика, металлургия и горнодобывающая промышленность, телекоммуникации, строительство, нефть и газ, услуги, гостиницы и рестораны, прочее» [13. С. 740–749]. В каждой из этих отраслей использовались разные технологии управления персоналом. Например, анализ персонала используется компаниями из транспортного, энергетического, телекоммуникационного и нефтегазового секторов. Электронное обучение сотрудников используется в сфере розничной торговли, транспорта, нефтегазового сектора. В совокупности было определено несколько цифровых технологий управления персоналом, включая, например, автоматизацию рабочих мест, электронное обучение, электронный набор персонала, гибкие методологии, управление талантами и т. д.

Следует отметить, что 15 % респондентов отказались от ненужного администрирования и используют современные технологии вместо бумажной волокиты. Но только 5 % компаний смогли автоматизировать расчеты. Равное число (5 %) компаний внедрило электронную аттестацию сотрудников. Даже 4 % компаний вообще не оценивают эффективность работы сотрудников, и только 2,5 % компаний используют персональные анкеты. 4 % компаний стараются избегать личного собеседования при выборе нового сотрудника. Такое же количество компаний (4 %) не оценивают сотрудников даже в рамках ежегодной оценки эффективности. И даже 3 % компаний рассматривают возможность полного прекращения кадрового учета.

Результаты анкет показывают, что 59,6 % респондентов осведомлены о положительном и отрицательном влиянии цифровизации на эффективность их работы. Остальные 40,4 % говорят, что цифровизация оказывает только положительное влияние на их рабочее место. В заключительной части статьи нами будут рассмотрены проблемы трансформации рабочего места в условиях цифровизации трудовых процессов. Среди положительных факторов респонденты отметили ускорение и упрощение производственного процесса, экономию времени, улучшение общения с коллегами, повышение гибкости, простой доступ к информации и т. д.

Напротив, они включили в число негативных проблем со здоровьем, связанных с работой с персональными компьютерами (ПК), ухудшение зрения, снижение или отсутствие физической активности и зависимость от современных технологий. Удивительно, но целых 86 % респондентов боятся вынужденных простоев, которые будут вызваны отключениями электроэнергии или «зависанием» современных технологий. Более половины респондентов (52,6 %) опасаются, что пожилые люди

потеряют работу из-за того, что не захотят учиться пользоваться современными технологиями.

Конкретным примером цифровизации в этом исследовании является Российский экономический университет имени Г. В. Плеханова, в котором обучается более 50 000 студентов. Они хотят внедрить цифровизацию для эффективной внутренней коммуникации, автоматического обмена информацией, снижения операционных затрат, а также для повышения эффективности сотрудников [5. С. 42–46; 8. С. 56–64].

Как отмечалось ранее, исследование, проведенное сотрудниками НИИ «Новая экономика и бизнес» показывает, что большинство респондентов положительно оценивают внедрение новых современных технологий в высшем образовательном учреждении. Хотя некоторые из них также обеспокоены негативными последствиями, особенно для их здоровья. Однако даже это не мешает им использовать эти новые технологии в своей работе. Положительные стороны перевешивают возможные отрицательные, поэтому и в образовательных учреждениях не следует бояться внедрять новые технологии, которые приносит Индустрия 4.0.

Проведенные исследования еще раз указывают на важность современных технологий в развитии человеческого капитала. Поскольку влияние технологий незаменимо, человеческий капитал должен развиваться вместе с технологиями. Каждая компания, которая желает быть конкурентоспособной, знает, что она должна нанимать лучших сотрудников, обладающих необходимыми знаниями и навыками. Поэтому большое внимание уделяется отбору, найму, управлению и оценке сотрудников. Эти процессы связаны технологией, поэтому важно отслеживать влияние технологий на человеческий капитал.

Следует указать на важность использования современных технологий при приеме на работу новых сотрудников. Электронный набор персонала более эффективен и интересен, чем классический. Кандидаты уже отправляют свою информацию в электронном виде при обращении в компанию. Таким образом, компания может определить, обладает ли рассматриваемый кандидат хотя бы базовыми навыками работы с компьютером. Различные коммуникационные платформы, такие как Skype, MS Teams, Google Meets, использовались для интервью во время болезни COVID-19.

В области повышения квалификации можно использовать эти современные технологии, например, для обучения и курсов для сотрудников. Сотрудники имеют доступ к учебным материалам в электронном виде, они могут участвовать в курсе через онлайн-платформы, поэтому не имеет значения, где они находятся.

Использование современных технологий в процессе управления человеческим капиталом – это появление электронного управления персоналом. Оно включает в себя онлайн-оценку эффективности работы сотрудника. Менеджер имеет доступ к данным также как и сотрудник. Однако критики e-HRM указывают на отсутствие письменных доказательств. С другой стороны, позитивно то, что административные расходы компании снижаются.

Важность информационно-коммуникационных технологий возросла в то время, когда мир страдает от COVID-19 [4. С. 33–37; 6. С. 163–168].

Поскольку одним из основных элементов Индустрии 4.0 является Интернет вещей и цифровизация, данное исследование сосредоточено на этих двух столпах.

COVID-19 также высветил неподготовленность людей к цифровым знаниям и навыкам. С его приходом люди со всего мира начали работать из дома в форме домашнего офиса. Студенты обучались дистанционному обучению на дому только с помощью ИКТ, а покупки также совершались онлайн.

Таким образом, проведенное исследование указывает на влияние широкополосной связи на человеческий капитал и общий объем производства в экономике. Через Интернет людям легче учиться, потому что у них есть доступ к различным учебным материалам и пособиям. Работа также становится проще, потому что ее можно выполнять в любое время и в любом месте, вам просто нужно иметь информационно-коммуникационное устройство с подключением к Интернету, и человек может работать, например, из автомобиля или зала ожидания у врача.

Россия нуждается в высококвалифицированных работниках с необходимыми цифровыми навыками для создания единого цифрового рынка и конкурентоспособного континента. Образование считается источником человеческого капитала, и оно позволяет достичь экономического успеха как отдельным лицам, так и компаниям.

Однако цифровые знания и навыки граждан России отстают от запланированных целей цифровизации. Опросы показывают, что многие лица в трудоспособном возрасте в России не могут найти подходящую работу, потому что у них нет необходимых знаний и навыков. Существует также проблема с рабочей силой со стороны работодателя. Целых 40 % компаний не могут заполнить вакансии, потому что они не могут найти подходящих кандидатов.

Несмотря на эти негативные сообщения, только четверо из десяти взрослых заинтересованы в образовании, дополнительной подготовке, курсах и обучении, которые им предлагаются. Этот факт также влияет на недостаточные цифровые знания и навыки сотрудников банковских учреждений или рабочих на заводах (до 37 % из них не обладают необходимыми знаниями).

Исследование показало значительное влияние технологий индустрии 4.0 на рынок труда, рабочие места и человеческий капитал, но авторы пришли к выводу, что автоматизировать большинство рабочих мест пока невозможно. Это может быть связано с нехваткой средств для приобретения современных технологий или нехваткой высококвалифицированного персонала, обладающего необходимыми цифровыми знаниями. Наличие на рынке труда рабочей силы, обладающей необходимыми знаниями, в определенной степени также определяется правительством, соответственно органами, которые разрабатывают учебные планы, планы аккредитации, проводят экономическую политику и т. д.

Важной проблемой для российской экономики является оценка влияния технологий индустрии 4.0 на трансформацию рабочего места в условиях цифровизации трудовых процессов [9. С. 457–462; 16. С. 283–290].

Респондентам был задан вопрос о важности раскрытия информации о рабочем месте и человеческих ресурсах как части раскрытия корпоративной социальной ответственности (КСО) внутренним и внешним заинтересованным сторонам. Все респонденты выразили положительное мнение о важности раскрытия подобной информации.

Результаты интервью показывают, что раскрытие информации о рабочем месте для внутренних и внешних заинтересованных сторон в основном делается для разных целей. Например, все опрошенные заявили, что сотрудники являются наиболее важной заинтересованной стороной и ценным активом в организации. Прозрачность информации о человеческих ресурсах для всех членов организации помогает компании построить хорошие отношения и сохранить наиболее ценный актив в бизнесе.

Достоверное раскрытие информации о том, как компания относится к сотрудникам и насколько хорошая рабочая культура в организации может стать хорошей стратегией для привлечения новых талантов, а также сохранить существующие таланты в организации.

Большинство опрошенных из группы сотрудников придерживались мнения, что это необходимо увидеть, независимо от того, раскрывается ли информация о рабочем месте и человеческих ресурсах внешним заинтересованным сторонам и, соответственно, приносит пользу компании. Если раскрытие информации принесет выгоды для компании, такие как привлечение новых инвесторов и улучшение корпоративного имиджа в глазах общественности, то информация должна быть раскрыта как внешним, так и внутренним заинтересованным сторонам. Однако, если раскрытие информации приносит больше вреда, чем пользы, то информация должна раскрываться только внутренним заинтересованным сторонам. Внутреннее раскрытие информации о рабочих местах и человеческих ресурсах повысит осведомленность сотрудников о развитии рабочего места и создаст доверие между сотрудниками, а также взаимное доверие с другими заинтересованными сторонами. Раскрытие также может мотивировать поощрять сотрудников к активному участию в мероприятиях, запланированных руководством для своих сотрудников, тем самым создавая хорошие отношения между руководством и сотрудниками.

Однако раскрытие информации о рабочих местах и человеческих ресурсах внешним заинтересованным сторонам важно для создания репутации и имиджа компании в глазах общественности, улучшения или продвижения «бренда работодателя», привлечения и поиска талантливых людей для работы в компании.

Интервьюируемых спрашивали о наиболее важных предметах/вопросах на рабочем месте и их предпочтение информации о человеческом капитале сосредоточилось на восьми категориях: корпоративная информация, трудовые отношения, вознаграждения работникам, вовлеченность персонала и трудовая жизнь, баланс, разнообразие и равные возможности, обучение и развитие, здоровье и безопасность. Исследование показывает, что с точки зрения управления они больше сосредоточены на вопросах, касающихся обучения и развития сотрудников, а также вопросах охраны здоровья и безопасности своих сотрудников, при этом сотрудники уделяют особое внимание льготам сотрудников, вовлеченности персонала и баланса между работой и личной жизнью.

В результате исследования установлено, что, с точки зрения работников, вопрос вознаграждения является самым важным вопросом, на который компания должна обратить внимание. Однако, помимо этого, сотрудники также обеспокоены вопросами обучения и безопасности, а также вопросом вовлечения.

В заключительной части статьи приведем результаты исследований, касающихся оценки уровня информационной безопасности России в современных условиях.

В настоящее время безопасность информации занимает важное и приоритетное место как для обеспечения национальной безопасности России в результате стремительного развития информационно-коммуникационных технологий и внедрения цифровой экономики, так и для предотвращения возникновения угроз безопасности граждан и государства, и повышения качества жизни современного российского общества [1].

Внедрение и применение цифровой среды предусматривает необходимость от всех участников процесса (государство, бизнес сообщество, наука, образование) определенного участия в стратегическом изменении существующей модели автоматизации. Стремительное развитие и внедрение компьютерных технологий, другими словами технологическая революция, объединило воедино различные системы (цифровые, физические, биологические и др.) и способствовало полному изменению в управлении экономикой. Такое преобразование, объединение и перерождение базируется, формируется и взаимодействует друг с другом в цифровой инфраструктуре [14].

Такая трансформация имеет тотальный характер и дает предпосылки к новым угрозам, которые могут влиять на трудовую систему отношений, на различия в уровнях доходов, на социальную этику и ценности. На рис. 1 показано место России в мировом рейтинге развития цифровой экономики за 2020 г.

Благодаря совершенствованию цифровых технологий становится легче получить информацию и возможность ее использования в части мирового бизнеса, а также к кадровым источникам и инновациям. Вследствие чего появляется возможность прогнозирования развития событий и, соответственно, эффективного планирования мирового рынка.

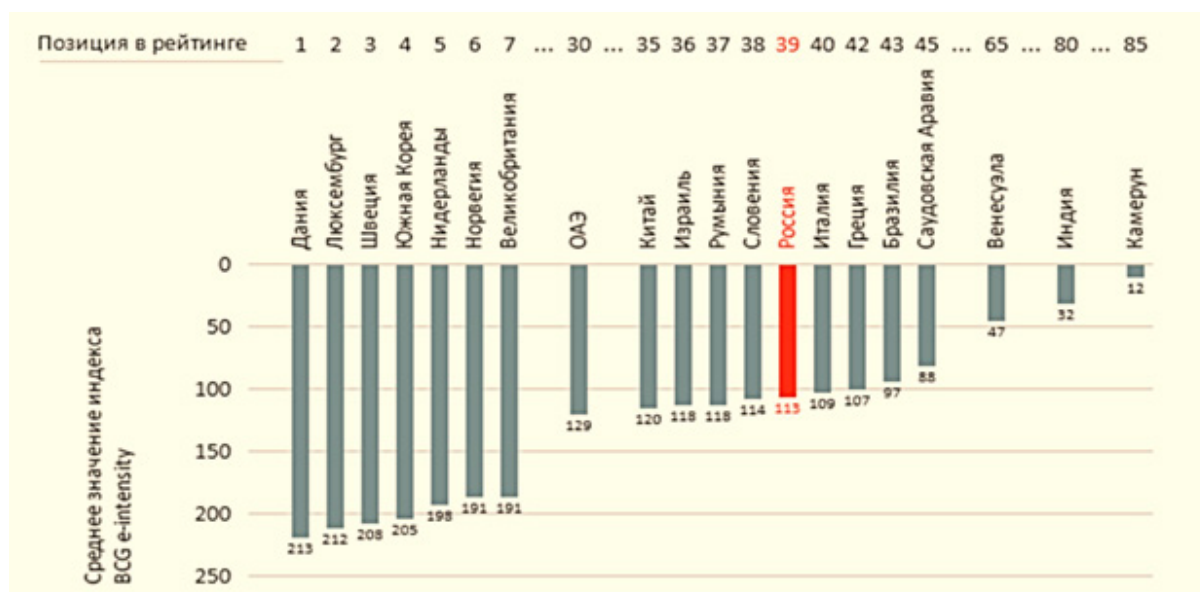


Рис. 1. Рейтинговое место России в цифровизации национальной экономики

Источник: [7. С. 187–196].

Несомненно, цифровизацию экономики можно назвать очередным и важным маркером глобальной экономики, который дает новый толчок для развития бизнеса и, соответственно, стимулирует к увеличению доходности и к увеличению заработка. Поэтому улучшение, усовершенствование и модернизация цифровой экономики – это новая основная реперная и дискуссионная точка в различных научных и социальных сообществах.

В настоящее время мировое сообщество обеспокоено сегодняшним положением в части защищенности национальных информационных ресурсов, а также возможностей через открытые информационные сети доступа к ним. Не существовавшие ранее вызовы и угрозы экономической безопасности, которые имеют отношение к цифровизации экономики, способны оказывать влияние на самостоятельность бизнеса, а также на способность предприятий конкурировать, и в целом несут угрозу безопасности государства в сфере информации.

Информационная безопасность должна обеспечивать защиту всех личных данных собственника и пользователя и предотвращать всякое вредоносное несанкционированное вмешательство извне к этим данным. [2. С. 547–570]. В связи с этим разрабатываются мероприятия, направленные на защиту информации, и в первую очередь, от компрометации конфиденциальности, целостности и доступности.

Наращивание множеством зарубежных стран способностей информационно-технического влияния на информационную структуру в военных целях является важнейшим отрицательным фактором, который оказывает воздействие на состояние информационной безопасности. Произошло увеличение числа утечек во всем мире относительно 2018 г. на 10 %, в России – свыше чем на 40 % [11].

На 51 % увеличилось в 2020 г. число уникальных киберинцидентов, если сравнивать с 2019 г. (рис. 2, 3).

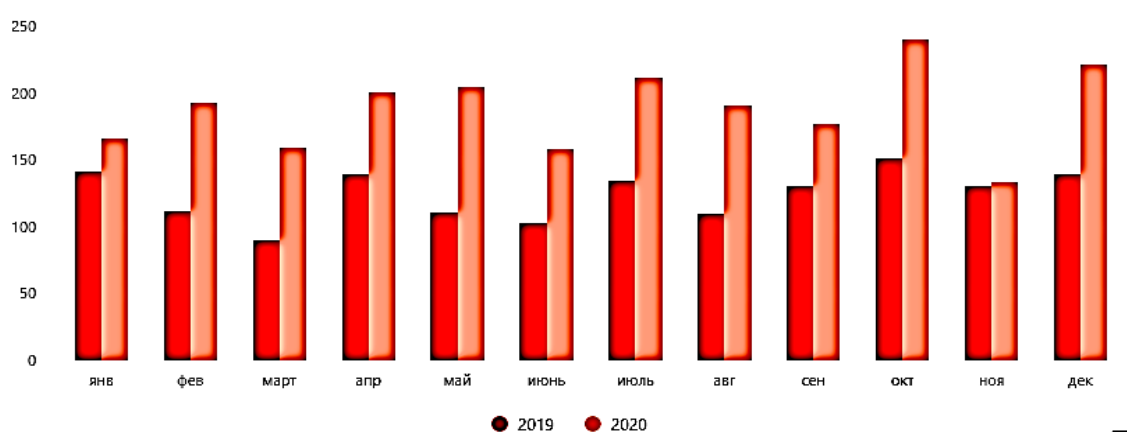


Рис. 2. Количество инцидентов в 2019 и 2020 гг.

Источник: [1].

70 % киберинцидентов имеют целенаправленный характер. Самыми популярными являются государственные структуры, медицина и промышленность.

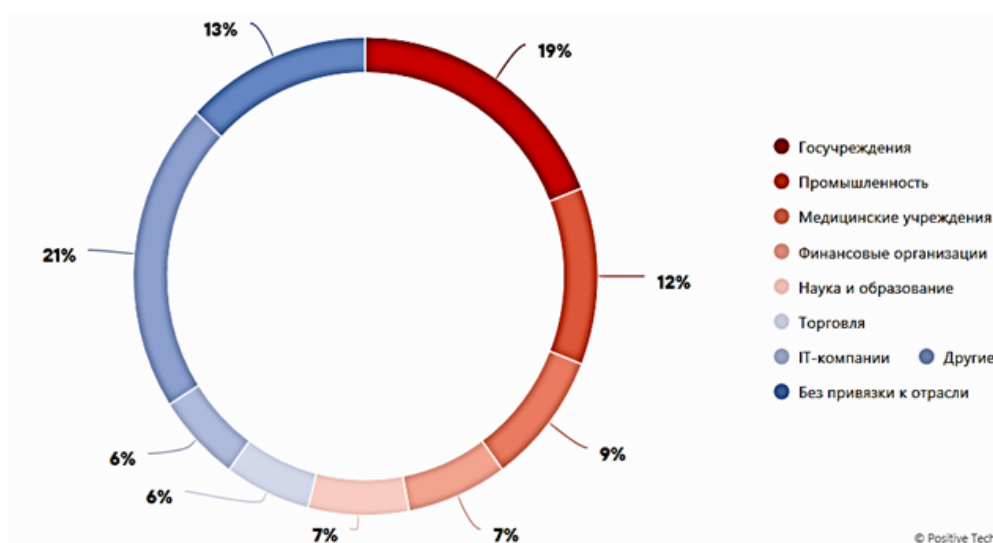


Рис. 3. Категории организаций, ставших жертвами атак
 Источник: [1].

Совет безопасности РФ, согласно главным целям его работы, формирует стабильные межведомственные комиссии, способные предотвращать внешние и внутренние угрозы, возникающие на функциональной или региональной базе.

Федеральной службой по техническому и экспортному контролю разработана и утверждена 05.02.2021 методика оценки угроз безопасности информации [12]. В документе приведен порядок, а также содержание работ, касающихся определения угроз безопасности информации. Они могут появляться в информационных системах, информационно-телекоммуникативных сетях, в системах АСУ (автоматизированная система управления), в других информационных инфраструктурах ЦОД (центров обработки данных) и облачных инфраструктурах.

Данный документ используется для того, чтобы выявить угрозы информационной безопасности, которые способны осуществляться в системах, а также сетях, привязанных к информационным системам различных государственных структур, системам, содержащим персональные данные, важным российским объектам в части информационной инфраструктуры, производственным системам управления.

Главные задачи, которые разрешаются в процессе оценки угроз безопасности информации – это [12]:

- а) выявление отрицательных результатов, которые способны появиться от осуществления угроз безопасности информации;
- б) инвентаризация систем, а также сетей и выявление возможных объектов влияния угроз безопасности информации;
- в) выявление источников угроз безопасности информации, а также оценка способностей нарушителей по осуществлению угроз безопасности информации;
- г) оценка методов осуществления угроз безопасности информации;
- д) оценка способности осуществления угроз безопасности информации, а также выявление актуальности угроз безопасности информации;

е) оценка схем осуществления угроз безопасности информации в системах, а также в сетях.

Совокупная схема реализации оценки угроз безопасности информации представлена на рис. 4.

В «Стратегии экономической безопасности РФ на период до 2030 года» представлен термин и закреплено понятие экономической безопасности. Кроме этого, сформирован новый список индикаторов, принимается во внимание важность мониторинга [10].

Что касается «Стратегии национальной безопасности Российской Федерации», то главной ее задачей считается комплекс трудов органов власти разных иерархических ступеней и общественных институтов для формирования необходимых внешних и внутренних условий для осуществления интересов государства, стратегических национальных инициатив, а также приоритетов. Основная же ее цель – обеспечение противоборство вызовам, а также угрозам экономической безопасности РФ, предупреждение и прогнозирование напряженных периодов в финансовой, научно-технологической, производственной и сырьевой областях.

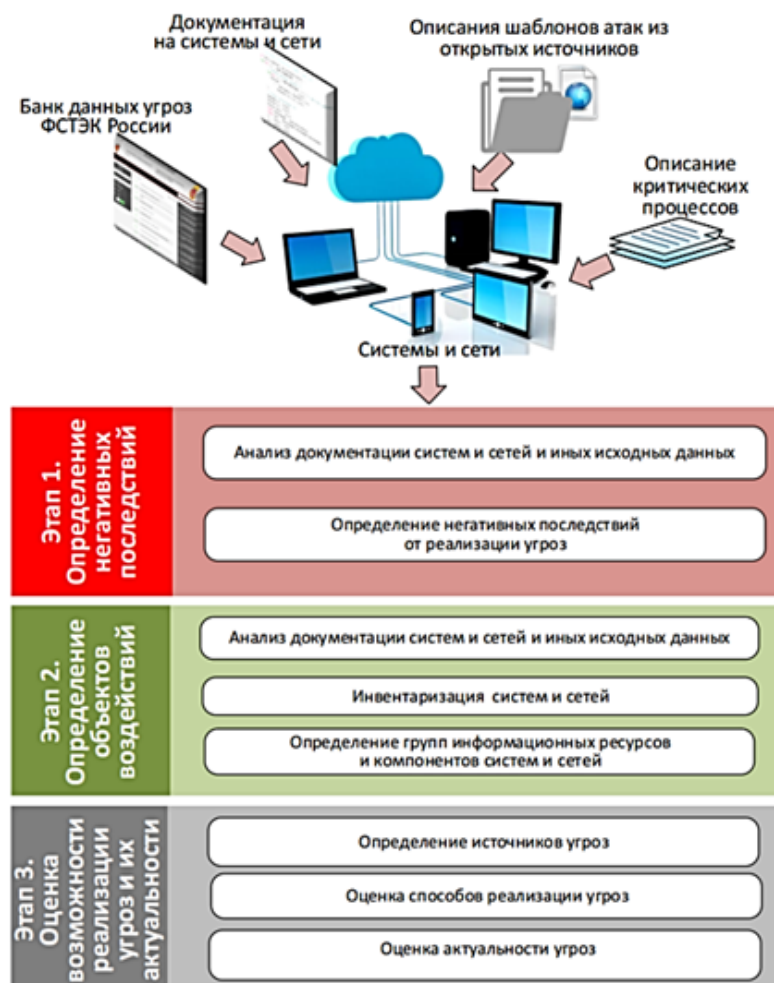


Рис. 4. Совокупная схема реализации оценки угроз безопасности информации

Для оценки экономической безопасности страны необходимы [3, 15]:

- отслеживание величин (показателей), которые являются основными в экономике и впоследствии провести сравнение этих величин с усредненными показателями глобальной (мировой) экономики, соответственно принимая их как пороговые значения;

- оценка скорости роста экономики государства по базовым макроэкономическим критериям и ходу развития их трансформации;

- способы оценки экспертов, которые необходимы для описания качественных, а также количественных характеристик рассматриваемых процессов. Это дает возможность на основе экспертных мнений осуществлять отбор правил и решений и дает возможность более глубокого познания в определенном проблемном секторе. Таким образом, есть возможность оценить степень кризиса в балльной системе и сгруппировать субъекты по угрожающей ситуации, ее степени (уровню), определяя индикаторы безопасности экономики по определенным правилам, которые основаны на их изучении и мониторинге.

Мерами по снижению действия негативных последствий по обеспечению информационной безопасности России также является: постоянное и непрерывное обновление мероприятий в части взаимного участия всех структур, обеспечивающих защиту в информационном секторе, чтобы быть готовыми к различным угрожающим ситуациям и к их предотвращению.

Важную роль имеют также мероприятия, направленные на обучение специалистов. Образование, подготовку персонала и повышение осведомленности в секторе по обеспечению защиты информации необходимо определить и популяризировать на глобальном, региональном и национальном уровнях.

Поэтому в России и установлен такой порядок, ежегодно соответствующие руководители, отвечающие за обеспечение безопасности страны, докладывают Президенту России о состоянии дел в части обеспечения национальной безопасности и том, что предпринимается для ее повышения и улучшения.

Заключение. Основываясь на анализе и сравнении научных исследований, мы обнаружили, что готовность к индустрии 4.0 и ее основам со временем изменилась. В начале (в 2016 г.) лишь немногие российские компании были готовы к индустрии 4.0 и цифровизации. Этот факт также подтверждается опросом, проведенным сотрудниками НИИ «Новая экономика и бизнес» РЭУ им. Г. В. Плеханова и группой российских ученых под руководством профессора Е. А. Федоровой, в котором отмечается, что в 2018 г. до 15 % компаний смогли использовать цифровизацию, хотя и только в управлении человеческим капиталом [13. С. 740–749].

Общей чертой всех проанализированных исследований был человеческий капитал и инвестиции в него в форме образования. В каждом исследовании подчеркивалась необходимость повышения квалификации и переподготовки сотрудников в результате внедрения элементов индустрии 4.0, независимо от страны. Этот факт не отличался в опросах 2021 г.

В статье подчеркивается, что разные компании по-разному относятся к индустрии 4.0. У них также есть различные условия для внедрения цифровизации на своих предприятиях. Важным выводом было то, что если бизнес хочет развиваться технологически, он не должен забывать о человеческом капитале. Именно

благодаря человеческому капиталу компании могут расти и получать конкурентные преимущества. Важно отслеживать и развивать человеческий капитал, потому что, если в компании не будут работать сотрудники с цифровыми навыками, компания не сможет использовать современные технологии.

Список литературы

1. Актуальные киберугрозы: итоги 2020 года. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/> (дата обращения: 24.07.2022).
2. Гретченко А. И., Гретченко А. А. Технологическая безопасность России: современное состояние, угрозы и способы обеспечения // Экономическая безопасность. 2022. Т. 5. № 2. С. 547–570. DOI: 10.18334/ecsec.5.2.114429
3. Гретченко А. И., Гретченко А. А. Проблема неравенства доходов населения и направления ее преодоления в системе национальной экономической безопасности. Высшая школа: научные исследования: материалы Межвузовского международного конгресса (г. Москва, 3 февраля 2022 г.). Москва: Инфинити, 2022. 72 с. DOI 10.34660/INF.2022.52.34.001
4. Гретченко А. И., Гретченко А. А. Управление человеческими ресурсами и кризис COVID-19: последствия, проблемы, возможности и будущие организационные направления // Финансовый бизнес 2022. № 5 (часть 1). С. 33–37.
5. Гретченко А. И., Гретченко А. А. Вузовская наука: проблемы, перспективы научно-технологического развития: материалы II Международной научно-практической конференции на тему: «Экономика и менеджмент промышленности: проблемы и современные решения». Ташкент, 2022. С. 42–46.
6. Гретченко А. И., Гретченко А. А. Организация рабочих мест в условиях удаленной занятости // Материалы докладов XXVI международной научно-практической конференции «21 век: фундаментальная наука и технологии», 18–19 мая 2021 г. North Charleston, Publisher: Lulu Press, Inc. 627 Davis Drive, Suite 300, Morrisville, NC. USA, 2021. С. 163–168.
7. Ерохина Е. В., Ерохин И. И. Риски информатизации и интеллектуализация в системе информационной безопасности Российской Федерации // Экономическая безопасность. 2020. Т. 3, № 2. С. 187–196.
8. Ерохина Е. В., Гретченко А. И. Риски и проблемы в условиях цифровизации российской экономики // Наука и практика. 2021. Т. 13, № 1 (41). С. 56–64.
9. Захаров Н., Кузнецов А., Бритвина И. Дилемма создания и потери рабочих мест перед индустрией 4.0. В: влияние индустрии 4.0 на создание рабочих мест. Б.и., 2019. С. 457–462.
10. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=389271#xxeO41TQp9PQHclS> 1 (дата обращения: 24.07.2022).
11. Утечки данных 2019: статистика, тенденции кибербезопасности и меры по снижению рисков взлома. URL: <https://www.vc.ru/services/103616-utechki-dannyh-2019-statistika-tendencii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma> (дата обращения: 24.07.2022).

12. Федеральная служба по техническому и экспортному контролю: Официальный сайт. URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhdenn-fstek-rossii-5-fevralya-2021> (дата обращения: 24.07.2022).

13. Федорова Е., Коропец О. и Гатти М. Цифровизация практики управления человеческими ресурсами и ее влияние на благосостояние сотрудников // Материалы Международной научной конференции «Современные проблемы в области бизнеса, менеджмента и экономики». Вильнюс, 2019. С. 740–749.

14. A. I. Gretchenko, A. A. Gretchenko (2019). The formation of the digital economy in Russian regions. II International Scientific Conference GCPMED 2019 “Global Challenges and Prospects of the Modern Economic Development” // European Proceedings of Social and Behavioural Sciences EpSBS. Pp. 430–436. DOI: 10.15405/epsbs.2020.03.62

15. Gretchenko Anatoly Ivanovich, Gretchenko Alexander Anatolyevich (2021). Quality of life of the Russian population: priorities of state policy, economic security of the country // Proceedings of the International Conference “Process Management and Scientific Developments” (Birmingham, United Kingdom, July 21, 2021). Part 2. Мельбурн: AUS PUBLISHERS, 2021. Pp. 8–15. DOI: 10.34660/INF.2021.76.30.001

16. Gretchenko A. I., Gretchenko A. A. (2021) Labor Market in the Conditions of Digitalization of the Russian Economy. In: Ashmarina S. I., Mantulenko V. V. (eds) Digital Economy and the New Labor Market: Jobs, Competences and Innovative HR Technologies. IPM 2020. Lecture Notes in Networks and Systems, vol. 161. Springer, Cham. https://doi.org/10.1007/978-3-030-60926-9_36. Pp. 283–290.

С. Д. Евсеева,
студент,

Российский государственный педагогический
университет имени А. И. Герцена

КОНЦЕПЦИЯ «УМНЫЙ ГОРОД» В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В настоящее время цифровые технологии оказывают значительное влияние на возникновение и становление различных отраслей. Именно благодаря содействию и совершенствованию данной сферы деятельности появляется все больше инновационных возможностей. В данной работе рассматривается концепция умного города, особенности влияния на нее аспектов цифровизации; определяется значимость развития подобных проектов, раскрываются основополагающие понятия и сопутствующие мероприятия ее реализации; изучены ключевые моменты, этапы становления программы, нормативно-правовые акты, статистические данные, а также различные точки зрения по данной проблематике.

Ключевые слова: цифровые технологии, цифровизация, умный город, IQ городов, город технологий, инновации, городская инфраструктура, комфортная среда

THE CONCEPT OF “SMART CITY” IN THE CONTEXT OF THE DIGITAL TRANSFORMATION OF THE RUSSIAN FEDERATION

Abstract. Currently, digital technologies have a significant impact on the emergence and development of various industries. It is thanks to the promotion and improvement of this field of activity that more and more innovative opportunities appear. In this paper, we consider the concept of “Smart City”, as well as what impact the aspect of digitalization has on this issue. We determine the meaning and importance of the development of such projects, reveal the fundamental concept and accompanying implementation measures. We study the key points, stages of the formation of the program, regulations, statistical data, and also analyze different points of view on the issue of interest.

Keywords: Digital technologies, Digitalization, Smart city, IQ of cities, Technology city, Innovations, Urban infrastructure, Comfortable environment

Преобразование и совершенствование современных технологий, а также актуальных информационных решений позволяют совмещать информационную и городскую среду. Тем самым развивать и улучшать жилищный и социальный комплексы, изменяя уровень жизни населения в лучшую сторону. Инновационные решения, основанные на использовании цифровых ресурсов, представляют возможность реализовывать современные проекты, благодаря которым повышается комфортность окружающей среды. Данные нововведения способствуют увеличению численности населения, так как удобство и доступность инфраструктуры является одним из важнейших условий для современных городских жителей.

Основываясь на учебном пособии «Основы цифровизации государственного и муниципального управления» [7. С. 151–152], можно говорить о том, что к цифровым технологиям относят объединение всех видов компьютерных технологий, включая сопутствующее оснащение и необходимое снабжение. В целях введения цифровизации в общее пользование применяется понятие «цифровой трансформации», т. е. процесс интеграции цифровых технологий.

Так как исследование преимущественно направлено на изучение государственно-правовых отношений и использование технологических решений, рассмотрим следующий тезис. Цифровая трансформация региона – глубокие и всесторонние изменения в производственных и социальных процессах, связанные с заменой аналоговых технических систем цифровыми и широкомасштабным применением цифровых технологий [8]. Данная процедура позволяет совершенствовать не только производственную и экономическую сферу, также направлена на продвижение и модернизацию социально важных условий. Достаточно часто употребляется понятие «электронное правительство» – форма организации деятельности органов государственной власти, обеспечивающая за счет широкого применения цифровых технологий качественно новый уровень оперативности и удобства получения потребителями государственных услуг и информации о результатах деятельности государственных органов [8].

Такая практика является достаточно распространенной тенденцией во многих странах мира. Помимо интеграции современных технологий в жизнь населения, а также формирования более доступной и гибкой среды, повышается эффективность и самого управленческого аппарата. Значительное внимание уделяется формиро-

ванию и совершенствованию аспектам стратегического планирования, отслеживанию данных, выявлению актуальных и сопутствующих проблемных ситуаций. С появлением новых систем взаимодействия населения и государства, посредством электронных ресурсов увеличился коэффициент полезности предоставления социально значимых услуг.

По нашему мнению, электронное управление имеет множество плюсов, например:

- высокое понимание потребности населения, при помощи интернет-опросов и голосований;
- повышенную ориентированность на социальные запросы;
- реализацию безопасной и комфортной среды;
- удобство взаимодействия между гражданами и государством;
- улучшение технологических навыков и осведомленности обеих сторон;
- более открытые данные, которые позволяют уменьшить возникновение коррупционных связей;
- удобство, оперативность и комфорт использования. Так как многие услуги можно получить при помощи гаджетов и онлайн-сервисов;
- уменьшение загруженности административных учреждений.

В Российской Федерации подобные технологические решения отображены в Национальной программе «Цифровая экономика Российской Федерации» [6]. В данной программе представлены девять федеральных проектов, преимущественно направленных на устойчивое развитие и совершенствование информационной составляющей страны, создания конкурентной среды и привлекательности государства, а также его технологических решений в целом. Основные направления: нормативное регулирование, развитие инфраструктуры, безопасности, исследования искусственного интеллекта, информатизация государственного управления, повышение возможностей всеобщего доступа, оказание услуг в информационном пространстве, кадровые вопросы и их компетентность. На данные направления было выделено значительное количество средств, которые реализованы как при помощи федерального бюджетирования, так и благодаря внебюджетным источникам. Основной целью проекта является внедрение цифровых процессов в экономическую и социальную сферу, создание благоприятного климата для дальнейшей деятельности.

В октябре 2018 г. был дан старт реализации программы, уже к 2024 г. она должна показать свои результаты. На данный момент значительное количество задач успешно выполнено, а ее актуальность, необходимость и известность может отобразить опрос ВЦИОМ [2]. Всероссийский центр изучения общественного мнения поинтересовался у респондентов о том, насколько они осведомлены о проекте «Цифровая экономика». Результаты опроса, показаны на рис. 1.

Проанализировав полученные показатели, можно утверждать о том, что национальный проект на момент опроса (2021 г.) уже был достаточно известен и, соответственно, имел успех в продвижении. Из полученных результатов следует то, что государство развивается в верном направлении, при дальнейшем совершенствовании которого оно сможет добиться положительных итогов. Безусловно, улучшения невозможны без массовой поддержки со стороны граждан, именно

поэтому необходимо придавать более широким образом огласке подобные программы. Тогда государственная деятельность в области цифровизации смогла бы обрести большую популярность, поддержку, а самое главное – актуальность в урегулировании проблем, которые на самом деле беспокоят общество.

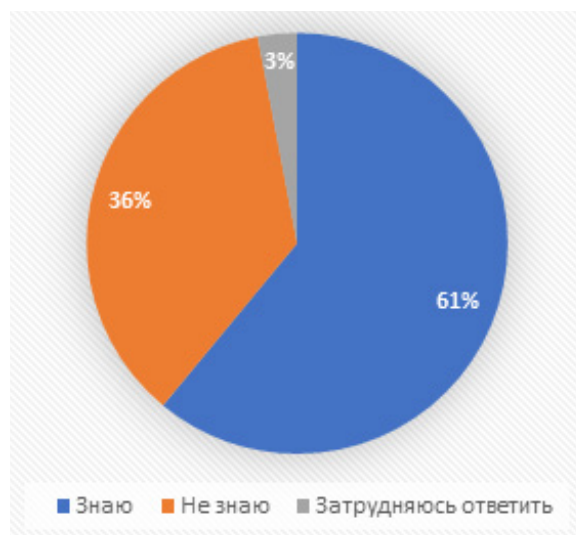


Рис. 1. Осведомленность граждан Российской Федерации о проекте «Цифровая экономика»

Как мы видим, цифровые изменения оказывают значительное влияние на государственно-правовые отношения и внутренние процессы. Именно поэтому на данный момент формированию и распространению информационных технологий уделяется такое пристальное внимание. С каждым годом появляется все больший объем данных, новые информационные решения проникают во все сферы жизни. Появляются больше возможностей в формировании и оптимизации жизненных направлений граждан, административных задач, в том числе в социально-экономической сфере. Для того чтобы следовать современным тенденциям многие страны по всему миру интегрируют инновации в повседневную жизнь горожан. Их использование помогает вывести государственное управление, а также все сопутствующие процессы на новый уровень.

Для того, чтобы поддерживать развитие современных концептуальных решений в жизнедеятельности граждан в Российской Федерации применяется концепция «Умный город». За ее реализацию отвечает Министерство строительства и жилищно-коммунального хозяйства РФ [3]. Его исполнение ведется в контексте выше изученной национальной программы [4], а также проекта «Жилье и городская среда» [5].

«Умный город» – это подход к развитию города использующего цифровые инструменты для повышения уровня жизни, качества услуг и эффективности управления при обязательном удовлетворении потребностей настоящего и будущих поколений во всех аспектах жизни. Такое определение указано в самом проекте [9], который был утвержден на период с 2018–2024 г. Также существует достаточно

много вариантов представления данного термина, например, с точки зрения цифровых систем, экономических, маркетинговых и многих других. Например, О'Грейди и О'Хара, автор книги «Насколько умен Ваш город?» [12. С. 1581–1582], говорят о том, что данное понятие слишком широко и какого-то конкретного описания для него не существует. Действительно, при рассмотрении подобной концепции, с различных точек зрения можно дать ей множество формулировок в зависимости от того, какую конкретно отрасль мы рассматриваем. Но все же анализируя государственное управление, мы придерживаемся мнения о том, что «Умный город» – это прежде всего реализация проектов, направленных на удовлетворение потребностей населения, посредством использования передовых цифровых технологий, в целях обеспечения высокого уровня комфортности и безопасности.

Основные приоритеты, которые заложены при задумке данного проекта, заключаются в создании комфортной и удобной атмосферы, безопасности и экологичности, эффективном управлении и постоянном совершенствовании. Для того чтобы сформировать и придерживаться всех вышеперечисленных принципов, создаются особые системы отслеживания информации, практического взаимодействия между государством и населением. Также для развития и поддержки инициативных проектов, реализуются мероприятия и особые программы, которые помогают раскрывать цифровой потенциал в стране.

Всего в проекте «Умный город», который реализуется на территории Российской Федерации, насчитывается 213 городов-первопроходцев, принимающих участие в цифровизации инфраструктуры социальной и экономической среды. Также для оценки качества внедрения информационных структур, введена особая система, позволяющая производить расчет эффективности. Она была запущена в 2018 г. и в конце 2024 г. мы сможем полномасштабно оценить результаты произведенной работы. Проанализировать то, насколько продуктивно была осуществлена деятельность по внедрению технологических процессов.

В целях обеспечения и реализации грамотной и отлаженной работы данного проекта были сформированы несколько основополагающих стандартов [1]. Стандарты включают в себя мероприятия, требования, сроки и предварительные результаты, благодаря которым становление информационной городской среды должно выйти на новый уровень. Мы проанализировали данные, представленные на официальном документе Министерства строительства и жилищно-коммунального хозяйства, выделили основные стандарты и сопутствующие методы, которые должны быть применены в целях достижения результата. Итоги обозначены в таблице.

Ключевые стандарты и требования к «умным городам», утвержденные Минстроем РФ показаны в таблице [1].

Таким образом, изучив планируемые цели, можно говорить о том, что при условии исполнения большинства мероприятий государство, а также его привлекательность во многом будет увеличена. Конкурентоспособность и возможность предоставления качественных государственных услуг, позволит не только улучшить качество жизни населения, но и представит возможным создать экономически-стабильную опору, которая будет функционировать не только за счет внутренних процессов, но и при помощи туристической сферы.

Установленные стандарты «Умного города»		
1	Управление городом	Реализация действий, преимущественно направленных на эффективную, результативную и грамотную работу государственных структур и оказываемых ими услуг.
2	Умное жилищно-коммунальное хозяйство	Обустройство систем, способствующих упрощению применяемых способов и сохранению ресурсов.
3	Городская среда – инновации	Применение цифровых методов, направленных на становление социально-экономического порядка и дальнейшего стимулирования развития.
4	Умный транспорт	Уменьшение количества аварийно-опасных ситуаций на дорогах, введение систем, способствующих оптимизации потока граждан в общественном транспорте.
5	Безопасность общества, инновационные системы	Мероприятия, направленные на устранение чрезвычайных ситуаций, улучшения контроля над уровнем безопасности населения, в том числе в информационном пространстве.
6	Экологическая среда, новые интеллектуальные методы	Использование новых возможностей для максимального уменьшения негативного эффекта нанесенного природе. Активное внимание в данном вопросе будет уделено сортировке отходов, чистоте воздуха, качеству воды.
7	Сетевая связь	Распределение нагрузки связующих линий, введение инновационных моделей, которые приведут к упрощению и увеличению пропускной возможности.
8	Туристическая система, сервис	Повышения активности туристов, путем введения методов, направленных на увеличение привлекательности городов, удобства передвижения, создания новых точек привлечения.

Изучая дальнейшее влияние, рассмотрим некоторые незатронутые сферы жизнедеятельности, и выявим уровень возможного цифрового влияния в них.

– Ресурсный потенциал. В современных реалиях ресурсное потребление достаточно велико, многие из них не восполняются и вскоре могут вовсе исчезнуть. В данном блоке можно выявить несколько проблем: нерациональное пользование природных запасов, а также экологический кризис. С учетом инновационного влияния, можно предложить создание эффективных и экономичных систем потребления, формирование возможности возобновления естественного потенциала. В целом, рационализация пользования сможет оказать положительное влияние.

Здравоохранение. Развитые страны по всему миру создают инновационные решения в области здоровья, борются со смертельными заболеваниями и сложными ситуациями. Цифровизация и финансирование данной области, является одной из самых приоритетных. Внедрение современных возможностей, позволят во многом преобразовать современные методы лечения, повысить квалификацию медицинского персонала. Кроме выше сказанного, информация поможет оптимизировать прием граждан и уменьшить загруженность учреждений, именно поэтому так важно развивать данное направление.

Образовательная система. Безусловно, учебные процессы всегда представляли особую ценность, именно они позволяют совершенствоваться и видоизменять дальнейшее будущее. Применение современных технологических решений, например,

таких как: улучшение мультимедийных возможностей, расширенное пользование интернет-систем, создание классов и аудиторий с использованием современных ресурсов и др. Именно они помогут вывести образовательную процедуру на совершенно новый и качественный уровень. Что в дальнейшем положительно отразится на развитии страны и ее возможностях.

Говоря о информатизации и совершенствовании процессов, нельзя не упомянуть в целом об объеме работ, которые были совершены на протяжении зарождения и их активного развития внутри страны. Для того, чтобы проанализировать влияние инновационных систем на Российскую Федерацию, мы обратились к данным Росстата [11] за 2010–2021 гг. В которых указано количество затраченных средств на реализацию товаров и услуг в целом. На основе изученных материалов, мы составили диаграмму, которая показывает финансовую динамику за 11 лет.

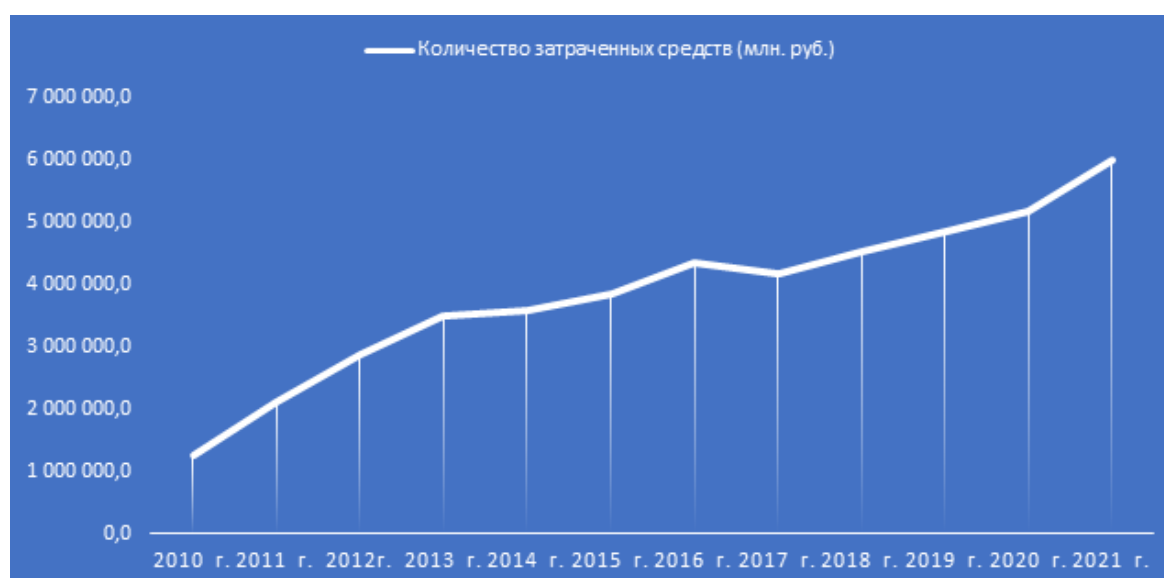


Рис. 2. Общие затраты на инновационные товары и услуги в период с 2010 по 2021 г. [11]

На диаграмме можно заметить то, что с 2010 г. показатели значительно выросли, практически достигнув значения пяти миллионов рублей. Безусловно данная тенденция является положительной, ведь именно она отражает то, насколько население и государство готово к информатизации общества. Особое внимание необходимо уделить периоду с 2018 по 2021 г., именно в этот промежуток времени началась активная поддержка цифровизации и реализация мероприятий по ее распространению. Даже несмотря на эпидемиологическую обстановку в стране с 2019 г., затраты на инновационную деятельность продолжали увеличиваться. Таким образом, мы можем сделать вывод о том, что меры по популяризации новых технологических процессов и решений являются достаточно актуальными, а также пользуются спросом у населения.

Также ранее мы упоминали про методику оценивания «IQ городов», которая была специально сформирована для проекта «Умный город». Главной особенностью

стью данного рейтинга, является распределение участвующих городов на четыре основные категории, в соответствии с количеством их населения, а также учета 47 показателей (основополагающие стандарты и их внутренние составляющие). В предшествующем 2021 г. [10] лидирующие позиции в категории крупнейшие города заняли: Москва, Санкт-Петербург, Нижний Новгород.

Использование данной методики дает возможность оценить настоящее положение и уровень цифровой трансформации. Одним из главных плюсов применения подобного расчета является групповое распределение, что позволяет ознакомиться с более точными и подробными результатами исследования, также выявить основные проблемные ситуации и слабые места при реализации проекта умного городского пространства.

В заключение хотелось бы сделать вывод о том, что цифровизация затрагивает все сферы жизнедеятельности людей, постепенно захватывая каждую область функционирования. На данный момент проект «Умный город», уже показал себя достаточно эффективной и результативной программой. Исходя из полученных статистических сведений, можно определить то, что при дальнейшей активной поддержке развития изучаемого направления, страну ожидают множество положительных инновационных открытий. Формирование комфортной и безопасной общественной сферы, является приоритетным направлением для каждой страны. Именно поэтому стоит уделять внимание совершенствованию, финансированию и формированию технологических компетенций в рамках социально-экономического развития.

Список литературы

1. Базовые и дополнительные требования к умным городам (стандарт «Умный город»). URL: <https://www.minstroyrf.gov.ru/upload/iblock/74f/Standart.pdf> (дата обращения: 03.09.2022).

2. ВЦИОМ–СПУТНИК – ежедневный всероссийский телефонный опрос ВЦИОМ. «Слышали Вы о национальном проекте в соответствующей сфере или нет? Цифровая экономика». URL: https://bd.wciom.ru/trzh/print_q.php?s_id=323&q_id=33913&date=04.04.2021 (дата обращения: 27.08.2022).

3. Дорофеева Л. В., Рослякова Н. А. Концепция умных городов как инструмент формирования умной специализации регионов: монография. Санкт-Петербург: Скифия-принт, 2019. 150 с.

4. Министерство строительства и жилищно-коммунального хозяйства Российской Федерации. URL: <https://www.minstroyrf.gov.ru/> (дата обращения: 28.08.2022).

5. Паспорт национального проекта «Жилье и городская среда». URL: <http://static.government.ru/media/files/i3AT3wjDNyEgFywnDrcrnK7Az55RyRuk.pdf> (дата обращения: 28.08.2022).

6. Паспорт Национальной программы «Цифровая экономика Российской Федерации» «Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации». URL: <https://digital.gov.ru/uploaded/files/programma.pdf> (дата обращения: 27.08.2022).

7. Полюшкевич О. А., Журавлева И. А., Дружинин Г. В., Москвитина Н. В. Основы цифровизации государственного и муниципального управления: учеб. пособие. Иркутск: Издательство ИГУ, 2020. С. 151–152.

8. Приказ Минкомсвязи России от 01.08.2018 № 428 «Об утверждении Разъяснений (методических рекомендаций) по разработке региональных проектов в рамках федеральных проектов национальной программы «Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_343571/1d43a52e7b24a093e2405a6520be0fa5394ebd09/ (дата обращения: 26.08.2022).

9. Приказ об утверждении Концепции проекта цифровизации городского хозяйства «Умный город». URL: https://www.minstroyrf.gov.ru/upload/iblock/315/25.12.2020_866_pr.pdf (дата обращения: 28.08.2022).

10. Результаты оценки хода и эффективности цифровой трансформации городского хозяйства РФ (IQ городов) по итогам 2021 года. URL: <https://www.minstroyrf.gov.ru/upload/iblock/672/REZULTATY-OTSENKI-KHODA-I-EFFEKTIVNOSTI.pdf> (дата обращения: 04.09.2022).

11. Федеральная служба государственной статистики (Росстат). URL: <https://rosstat.gov.ru/statistics/science> (дата обращения: 03.09.2022).

12. O'Grady M., O'Hare G. How Smart Is Your City? // Science. 2012. № 3. Vol. 335. Pp. 1581–1582.

А. В. Еремеева,
магистрант,

Волгоградский государственный университет

ЦИФРОВИЗАЦИЯ В СФЕРЕ ГОСУДАРСТВЕННЫХ ЗАКУПОК: ПРЕТЕНЗИОННАЯ РАБОТА КАК ЧАСТЬ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Аннотация. В статье рассматриваются проблемы реализации Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» в части ведения претензионной работы при осуществлении государственных закупок. Проанализированы оптимизационные нововведения по данному направлению, вступившие в силу с 1 июля 2022 г. Также установлена роль претензионной работы в системе электронного документооборота закупочной деятельности. Целью настоящего исследования является анализ механизма реализации претензионной работы при исполнении государственных контрактов федеральных заказчиков. Методы: использованы методы системного и сравнительно-правового анализа. Результаты: обоснованная в работе авторская позиция опирается на законодательство, результаты исследования специалистов по вопросу применения механизма ведения претензионной работы. В статье изложены краткие выводы по совершенствованию механизма реализации ведения претензионной работы при исполнении государственных контрактов. Учитывая важность бесперебойного выполнения государственного заказа, законодатель позаботился о системе мер по соблюдению баланса между защитой интересов государственного заказчика и исполнителя. Одним из важных механизмов защиты прав обеих сторон является реализация досудебного урегулирования гражданско-правовых споров. Ведение претензионной работы позволяет

решать гражданско-правовые споры при осуществлении государственных закупок в более короткие сроки и минимизировать потери государственных заказчиков.

Ключевые слова: цифровые технологии, государственные закупки, претензионная работа, электронный документооборот, единая информационная система, «оптимизационные» поправки, контрактная система, государственный контракт

DIGITALIZATION IN THE FIELD OF PUBLIC PROCUREMENT: CLAIM WORK AS PART OF ELECTRONIC DOCUMENT MANAGEMENT

Abstract. The article deals with the problems of implementation of Federal Law “On the contract system in the procurement of goods, works, services for state and municipal needs” in terms of conducting claim work in public procurement. Optimization innovations in this area, which entered into force on July 1, 2022, have been analyzed. The role of claim work in the electronic document management system of procurement activities is also established. The purpose of this study is to analyze the mechanism of implementation of claim work in the execution of state contracts of federal customers. Methods: methods of consistency, analysis and comparative law are used. Results: the author’s position justified in the work is based on legislation, the results of a study by specialists on the application of the mechanism for conducting claim work. The article presents brief conclusions on improving the mechanism for implementing the conduct of claims work in the execution of government contracts. Given the importance of uninterrupted execution of the state order, the legislator took care of a system of measures to maintain a balance between protecting the interests of the state customer and the contractor. One of the important mechanisms for protecting the rights of both parties is the implementation of pre-trial settlement of civil law disputes. Conducting claims work allows you to resolve civil law disputes in the implementation of public procurement in a shorter time and minimize the losses of government customers.

Keywords: Digital technologies, Public procurement, Claim work, Electronic document management, Unified information system, “Optimization” amendments, Contract system, Government contract

Введение. Цифровые технологии коснулись всех областей жизнедеятельности человека. Наиболее сильное влияние цифровизации наблюдается в экономической сфере. В экономике любого государства большую долю занимают государственные закупки, направленные на выполнение общенациональных задач, способствующие поддержанию жизнедеятельности и удовлетворению потребностей общества. Интеграция цифровых технологий экономической сферы и права способствует более четкому выполнению вышеуказанных задач. Одним из главных принципов государственных закупок является их законность [10. С. 75–80].

Сферу государственных закупок регламентирует Гражданский кодекс Российской Федерации, а также специальные федеральные законы. Причем во всем, что не урегулировано напрямую специальными законами, следует руководствоваться общими нормами гражданского законодательства [5. С. 250–308].

Основным специальным законом является Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – Федеральный закон от 05.04.2013 № 44-ФЗ). С момента вступления в силу Федерального закона от 05.04.2013 № 44-ФЗ законодателем регулярно вносились требуемые временем и экономической обстановкой изменения. Тем не менее самыми революционными изменениями стали «оптимизационные поправки», внесенные в контрактную систему Федеральным законом от 2 июля 2021 г. № 360-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». В этих поправках наиболее четко прослеживаются тенденции интеграции цифровизации и права в экономической сфере государственных закупок [8. С. 61–68].

Претензионная работа как часть электронного документооборота. Тенденция последних лет процесса цифровизации в сфере государственных закупок направлена прежде всего на упрощение и увеличение прозрачности закупочных процедур, на защиту экономических интересов участников и на снижение временных затрат. Внедрение в закупочный процесс электронного документооборота играет огромную роль для достижения вышеуказанных целей. Консолидация в единой информационной системе всего закупочного цикла от извещения до полного исполнения государственных контрактов, позволяет не только добиться максимальной прозрачности, но и значительно упростить работу участников государственных закупок, сокращая время и расстояние.

Масштабным процессом в плане цифровизации государственных закупок является внедрение в систему электронного документооборота электронной приемки или так называемого электронного активирования. Данный процесс ознаменовал окончание перевода процедур расходования бюджетных средств в электронную форму. Все стадии закупочного цикла, от размещения извещения до ведения реестра контракта стали практически полностью автоматизированными. Интеграция всех стадий закупочного процесса позволяет минимизировать ошибки, причиной которых является человеческий фактор. Данные из государственного контракта автоматически протягиваются в цифровой среде в универсальный передаточный документ, что исключает для исполнителей государственных закупок возникновение технических ошибок [6. С. 290–303].

Но исполнение контракта не всегда является конечным циклом государственной закупки, исполнители государственных контрактов могут допустить нарушения сроков поставки или исполнения работ, так же могут возникать гражданско-правовые споры по поводу качества исполненных обязательств и т. д. У государственных заказчиков нередко возникает необходимость расторгнуть контракт в одностороннем порядке. Глобальным изменением в этом направлении можно считать автоматизацию направления решения об одностороннем расторжении контракта в единой информационной системе. Сформированное решение автоматически направляется стороне и датой получения считается день публикации данного решения. Ранее решение о расторжении сторона направляла почтовым отправлением или еще каким-либо законным способом, например телетайпом или электронной почтой. Данный механизм ставил сторону в зависимость от третьих лиц, а именно почто-

вые направления могли занимать достаточно большой временной промежуток, адрес, в том числе электронный мог быть не действительным и т. д. Переход этого процесса полностью в цифровую среду данную проблему решил [4. С. 162–173].

Однако, прежде чем принять решение об отказе от контракта и расторжении, необходимо провести претензионную работу. Претензионная работа или досудебное урегулирование споров является действенным инструментом, позволяющим исчерпать возникшие разногласия, сохранить баланс интересов сторон и минимизировать затраты и потери. И самое главное позволяет сэкономить время, так как судебный порядок урегулирования споров представляется чрезмерно длительным и обременительным с финансовой точки зрения.

До недавнего времени специальных норм, регламентирующих порядок ведения претензионной работы в Федеральном Законе от 05.04.2013 № 44-ФЗ не было. Участники государственных закупок руководствовались, прежде всего Гражданским кодексом Российской Федерации (далее – ГК РФ) и Арбитражным процессуальным кодексом Российской Федерации (далее – АПК РФ).

ГК РФ устанавливает общие положения о разрешении гражданско-правовых споров и регулирует претензионный порядок в отношении конкретных видов сделок, а так же меры ответственности за неисполнение взятых на себя обязательств. В АПК РФ для всех гражданско-правовых споров установлен обязательный претензионный порядок разрешения споров.

Претензионная работа с точки зрения правовых средств представляет собой взаимоувязанные юридически обоснованные действия, направленные на досудебное урегулирование споров. Документальным обеспечением данных правовых средств является претензия с полным пакетом необходимых документов и ответ на нее. Сторона, чьи права нарушены, обязана предъявить должнику требование об исполнении возложенных на него обязанностей, должник должен ответить в установленный срок [2. С. 186–188].

В ГК РФ указано, что гражданско-правовые последствия наступают для лица, на которое возложены обязательства по сделке с момента доставки юридически значимых сообщений, в том числе претензий этому лицу либо его представителю [3. С. 506–507].

Направление претензионных документов осуществлялось следующими видами связи: почтовыми отправлениями (письмом заказным или ценным), по телеграфу, телетайпу, по электронной почте, а также нарочно и вручалось под расписку уполномоченному должностному лицу.

Направление претензий таким образом существенно тормозило оперативное решение споров в досудебном порядке, так как доставка претензионных документов могла занимать значительное время, кроме того могла быть безуспешной, например в случае недействительности почтового адреса по которому осуществлялось направление [1. С. 60–69].

С июля 2022 г. в Федеральном законе от 05.04.2013 № 44-ФЗ появилась отдельная норма об электронной претензионной работе. Согласно ч. 16. ст. 94 обмен претензионными документами осуществляется при помощи единой информационной системы путем направления через нее электронных уведомлений [9. С. 1651].

Таким образом, с введением этой нормы практически все взаимодействие сторон государственных закупок стало осуществляться в цифровой среде, в данном случае в Единой информационной системе. А юридически важные события, такие как подписание государственного контракта, приемка товара, работ или услуг, претензионная работа, расторжение или отказ от государственного контракта, подача жалоб в контролирующие органы происходит без участия третьих лиц, напрямую между заинтересованными сторонами в цифровой среде.

Выводы. Претензионная работа – это важная часть реализации правоспособности участников договорных отношений в области разрешения финансово-хозяйственных споров в досудебном порядке. Основной целью претензионной работы являются обеспечение договорной дисциплины между участниками договорных отношений и защита законными средствами имущественных прав и интересов сторон.

Возможность ведения претензионной работы в цифровой среде в форме электронного документооборота позволяет более эффективно осуществлять взаимодействие сторон государственных закупок при возникновении спорных моментов и в конечном итоге направлена как на безусловное исполнение государственных контрактов, так и на бесперебойное осуществление государственных закупок в целом.

Список литературы

1. Власов А. Б. Эффективность и совершенствование претензионной работы по госзакупкам / А. Б. Власов, К. И. Кремер // Современная экономика: проблемы и решения. 2021. № 8 (140). С. 60–69. EDN: ETJWZX. DOI: 10.17308/meps.2021.8/2654
2. Гаранина М. А. К вопросу об организации юридической службы претензионной работы // Молодой ученый. 2021. № 27 (369). С. 186–188. EDN: LWUNWV
3. Гражданский кодекс Российской Федерации. Части первая, вторая, третья и четвертая. Москва: Проспект, 2020.
4. Казакова Е. Б. Единая информационная система и единый агрегатор торговли «Березка» в системе государственных закупок и их правовое регулирование / Е. Б. Казакова, А. Ю. Шишкова // Наука. Общество. Государство. 2020. Т. 8, № 2 (30). С. 162–173. EDN: TRNFVY. DOI: 10.21685/2307-9525-2020-8-2-18
5. Кнутов А. В. Управление государственными и муниципальными закупками и контрактами: учебник и практикум для вузов. Москва: Юрайт, 2022. 316 с. (Высшее образование). ISBN 978-5-534-04912-1. URL: <https://urait.ru/bcode/492924> (дата обращения: 19.09.2022).
6. Овсянкин Д. Л. Анализ эффективности использования системы государственных закупок // Финансовые рынки и экономический рост: материалы Международной научно-практической конференции. Москва. 27–28 мая 2019 года. Москва: Перо, 2019. С. 290–303. EDN: WSCPNM.
7. Павлова А. С. Внедрение автоматизации ведения претензионной работы в сфере закупок // Инновации в сфере закупок: запрос рынка труда и профессионализм заказчиков: сборник научных докладов / отв. ред. И. П. Гладилина. Москва: ООО «Русайнс», 2022. С. 90–98. EDN: GXNKOS
8. Плотников В. А. Перспективы развития системы государственных закупок и государственного оборонного заказа / В. А. Плотников, С. И. Рогатин // Известия

Санкт-Петербургского государственного экономического университета. 2022. № 4 (136). С. 61–68. EDN: HGUUFL

9. Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // Собрание законодательства Российской Федерации от 8 апреля 2013 г. № 14. Ст. 1652.

10. Федорова И. Ю. Финансовый механизм государственных и муниципальных закупок: учебное пособие для вузов / И. Ю. Федорова, А. В. Фрыгин. Москва: Юрайт, 2022. 148 с. (Высшее образование). ISBN 978–5–534–10877–4. URL: <https://urait.ru/bcode/490365> (дата обращения: 19.09.2022).

М. М. Есиркепова,

PhD, доцент,

Astana International University / Michigan State University

ДИСТАНЦИОННАЯ РАБОТА В УСЛОВИЯХ ПАНДЕМИИ КОРОНАВИРУСНОЙ ИНФЕКЦИИ

Аннотация. В статье рассматриваются вопросы решения нестандартной формы занятости, отвечающей потребностям сложившейся ситуации в период коронавирусной инфекции. В трудовых отношениях одной из гибкой формы занятости является дистанционная работа, уже нашедшая законодательное закрепление в большинстве стран мира. Изложены актуальные вопросы трудового права Республики Казахстан и стран зарубежных республик. Объектом данного исследования являются правовые вопросы трудовой деятельности в условиях дистанционной работы. Целью научной работы выступает изучение актуальных вопросов и выявление различных потенциальных трудовых споров при переходе на дистанционную форму рабочей деятельности. Кроме того, определена профессиональная и правовая особенность наемных работников при переходе на удаленную форму.

Ключевые слова: трудовое право, трудовой кодекс Республики Казахстан, форма работы, дистанционная работа, пандемия

REMOTE WORK IN CONDITIONS OF CORONAVIRUS INFECTION

Abstract. The article considers the issues of solving a non-standard form of employment that meets the needs of the current situation during the coronavirus infection. In labor relations, one of the flexible forms of employment is remote work, which has already found legislative consolidation in most countries of the world. The article outlined topical issues of labor law of the Republic of Kazakhstan and the countries of foreign republics. the object of this research is the legal issues of labor activity in the conditions of remote work. The purpose of the scientific work is to study topical issues and identify various potential labor disputes during the transition to a remote form of work activity. In addition, the professional and legal features of employees when switching to a remote form are determined.

Keywords: labor law, Labor Code of the Republic of Kazakhstan, form of work, remote work, pandemic

В условиях пандемии трудовые отношения сформировались в новых правоотношениях между работодателем и работником. Работодатели положительно относятся к переходу своих сотрудников на удаленную работу, так как это позволяет продолжать деятельность компании, сокращать расходы как работника, так и работодателя. С другой стороны, работодателю было бы легче и удобнее координировать и контролировать работу в офисе, постоянно повышая эффективность труда своих сотрудников.

Королевский указ 28/2020 от 22 сентября («Закон 28/2020») вводит новое регулирование дистанционной работы в испанское законодательство. В постановлении, которое вступает в силу 13 октября 2020 г., уточняются определяющие условия удаленной работы и перечисляются права работников, оказывающих услуги через эту форму организации труда [1].

Закон 28/2020 определяет дистанционную работу как форму организации труда или осуществления трудовой деятельности, в соответствии с которой она осуществляется в доме работника или в выбранном им месте в течение всего или части рабочего дня на регулярной основе. В этом смысле удаленная работа понимается как «регулярная», когда в течение отчетного периода в 3 месяца на удаленную работу отводится не менее 30 % рабочего дня (или эквивалентный процент в контрактах на неполный рабочий день). С другой стороны, телеработа определяется как дистанционная работа, выполняемая исключительно или с использованием компьютерных, телепатических и телекоммуникационных средств и систем.

Прежде чем указывать характерные примечания, внесенные в корпус регламента, следует отметить, что Закон РД 28/2020 не применяется к следующим ситуациям удаленной работы:

а) удаленная работа, исключительно реализованная в качестве меры по сдерживанию кризиса в области здравоохранения, вызванного Covid-19;

б) ситуации удаленной работы, которые существовали до 13 октября 2020 г. и которые регулировались коллективными соглашениями или другими коллективными соглашениями, до тех пор, пока они не перестанут действовать.

Однако Закон 28/2020 действительно применяется к тем соглашениям об удаленной работе индивидуального характера, которые действовали на момент публикации постановления (22 сентября) и не вытекали из коллективных договоров или других коллективных соглашений. Поэтому работники, которые уже предоставляют свои услуги удаленно, должны оформить соответствующее соглашение или внести соответствующие изменения или изменения в действующие соглашения в течение 3 месяцев.

Закон 28/2020 вводит следующие принципы и формальные требования к предоставлению удаленных услуг:

Добровольная и обратимая: удаленная работа является добровольной как для работника, так и для компании, и поэтому не может быть навязана.

Ограничения: в трудовых договорах, заключенных с несовершеннолетними лицами, а также в договорах об обучении и ученичестве, удаленная работа возможна, если обеспечивается, что не менее 50 % услуг предоставляются на месте.

Формальности: соглашение всегда должно быть в письменной форме и может быть согласовано в начале трудовых отношений или в более позднее время. Любое изменение соглашения должно быть оформлено в письменной форме и согласовано с компанией или сотрудником, если это применимо. Компания также должна предоставить копию соглашения представителям сотрудников (в течение максимум 10 дней с момента его официального оформления), которые должны подписать его, чтобы подтвердить доставку. Затем эта копия соглашения должна быть отправлена в соответствующее бюро по трудоустройству.

Минимальное обязательное содержание соглашения:

- Инвентаризация активов, оборудования и инструментов, необходимых для осуществления деятельности (включая расходные материалы и мебель), с указанием срока их полезного использования или максимального периода обновления.
- Перечисление расходов и указание формы количественного определения компенсации, подлежащей выплате компанией, а также времени и формы ее выплаты.
- Часы работы и рекомендации по доступности.
- Рабочее место компании, к которой прикреплен сотрудник.
- Удаленное местоположение, указанное сотрудником.
- Продолжительность периодов уведомления для осуществления обратимости.
- Методы корпоративного контроля за деятельностью.
- Процедура, которой следует следовать в случае технических трудностей, препятствующих нормальной удаленной работе.
- Инструкции, изданные компанией с участием представителей сотрудников, по защите данных и информационной безопасности.
- Срок действия договора о дистанционной работе.

Наконец, следует отметить, что Закон устанавливает специальную правовую процедуру срочного и преференциального характера для жалоб на доступ, отмену и изменение удаленной работы.

Принятие Закона 28/2020 является важной вехой в регулировании труда, обновляя действующие нормативные акты и устанавливая четкие направления действий для работодателей и работников. Несмотря на положительные аспекты этого регулирования, норма не исчерпывает проблему, поскольку оставляет наиболее спорные элементы (например, компенсацию расходов) этой формы предоставления услуг в руках социальных агентов.

Трудовые отношения имеют свои особенности, позволяющие отличать их от смежных гражданско-правовых отношений в сфере использования наемного труда. Предметом трудовых отношений является трудовой процесс, в котором работодатель организует и обеспечивает защиту, а работник соблюдает установленные работодателем правила внутреннего трудового распорядка. Трудовые отношения основаны на личном характере трудовой деятельности работника с подчинением трудовым правилам. Компенсационный характер трудовых отношений проявляется в основной обязанности работодателя по своевременной выплате заработной платы наличными деньгами.

Ст. 23 Конституции устанавливает право всех граждан на свободу объединений и устанавливает, что деятельность общественных объединений регулируется законом. Профсоюзы в Республике Казахстан являются одним из видов общественных объединений граждан, созданных на добровольной основе для достижения общих целей, не противоречащих закону. Профсоюзы являются некоммерческими организациями, которые объединяются самостоятельно с добровольным членством.

По мере экономического развития республики проблема безработицы должна быть ослаблена, но полная ликвидация невозможна при наличии рынка труда. Такие выводы позволяют сделать опыт зарубежных стран, которые вышли на высокий уровень экономического развития, но не искоренили эту проблему в своем обществе. Уровень безработицы публикуется в США, как правило, в первую пятницу каждого месяца, в еврозоне данные по уровню безработицы выходят в первые десять дней каждого месяца, в Японии в конце месяца. Так, официально зарегистрированный уровень безработицы в процентах от экономически активного населения составил на конец 2016 г. в США – 4,6 %, в Казахстане – 5 %, в России – 5,4 %, Германии – 3,9 %, Великобритании – 4,8 %.

Таким образом, для перехода на удаленную работу необходимо соблюдать установленные законодательством требования по уведомлению работника, оформлению соответствующей документации, а также четко прописывать все условия удаленной работы в трудовом договоре и дополнительном соглашении во избежание разногласий с работником, работающим удаленно.

Несмотря на рассмотрение вышеуказанного проекта, регулирование удаленной работы в РК полностью не усовершенствовано. В связи с этим имеется необходимость проанализировать последние изменения в российском трудовом законодательстве.

Для тех сотрудников, чей бизнес позволяет это, удаленная работа является очевидным решением текущей ситуации, поскольку она позволяет бизнесу продолжать работать и, что немаловажно, сотрудникам сохранять свои рабочие места. Этот подход также был рекомендован Министерством труда и социального обеспечения.

Трудовой кодекс содержит обзор общего процесса удаленной работы, описывая его как процесс, при котором люди работают вне офиса, используя предоставляемые информационно-коммуникационные технологии. При работе удаленно обе стороны могут в письменной форме договориться о предусмотренной законом компенсации любых дополнительных расходов на сотрудников, связанных с этим.

Однако Трудовой кодекс не рассматривает работу вне офиса так же, как удаленную работу, поскольку последняя требует изменения методов работы и места работы, а это означает, что условия, регулирующие удаленную работу, должны быть включены в трудовой договор вместе со стоимостью любой соответствующей дополнительной компенсации.

Работодатели должны помнить, что удаленная работа вне офиса без соответствующих актов работодателя и поправок к трудовому договору не может рассматриваться как удаленная работа. В этом случае работник сохраняет за собой все свои права и обязанности по действующему трудовому договору, за исключением права на дополнительную компенсацию.

Важно отметить, что работодатели могут использовать механизм удаленной работы в своих интересах, поскольку он позволяет им нанимать иностранных граждан, которые не смогли въехать в Казахстан из-за чрезвычайного положения и карантинных мер, без необходимости обращаться за разрешением на работу.

Современные технологии, включая электронную документацию, как внутри компании, так и с третьими лицами, могут сократить контакты с сотрудниками и позволяют людям работать вне офиса, например, во время карантина. По закону оригиналами признаются документы, созданные в электронном виде и подписанные электронной подписью. Обмен электронными документами может осуществляться внутри компании с использованием любых информационных технологий или средств идентификации, в то время как обмен электронными документами с третьими лицами требует специальных платформ, позволяющих обеим сторонам создавать документы и подписывать их в электронном виде в соответствии с установленной законом процедурой. В настоящее время в Казахстане существует ряд таких платформ, и более подробную информацию о них вы можете найти на вебинаре «Делойта», посвященном обмену электронными документами [2].

Работодатели, чей бизнес не может приспособить механизм удаленной работы, могут:

- установить графики смен неполного рабочего дня, достаточные для выполнения санитарных мер по защите от инфекции, и в то же время ограничить количество сотрудников в офисе в любой момент времени;

- отправлять сотрудников в отпуск – как оплачиваемый (если у сотрудника есть свободные дни отпуска), так и неоплачиваемый. В то время как оплачиваемый отпуск должен снизить риск заражения из-за отсутствия работника в офисе, он не уменьшит финансовую нагрузку работодателя, поскольку он оплачивается исходя из среднемесячной заработной платы работника. Неоплачиваемый отпуск может уменьшить расходы работодателя, но предоставляется только с согласия работника.

Если работник не согласен взять неоплачиваемый отпуск, он будет иметь право на оплату простоя, независимо от его причины. Размер любой такой выплаты определяется трудовым или коллективным договором, но не должен быть меньше установленного законом минимального размера оплаты труда.

Увольнение – это крайняя мера, которая может привести к напряженности в этот сложный период, но, если работодатели вынуждены использовать ее в качестве стратегии, они должны заранее уведомить об этом за один месяц и в течение следующего года никого не нанимать на должности, которые были сокращены.

В заключение хотелось бы подчеркнуть, что в эти трудные времена и работники, и работодатели обязаны друг перед другом в максимально возможной степени не способствовать социальной напряженности и не усугублять и без того очень сложную ситуацию. Все стороны трудовых отношений должны попытаться использовать этот период для корректировки деловой среды и своего подхода к работе, а также найти время для поиска новых инновационных подходов

к повседневным бизнес-процессам. Считаем, что ключевые шаги, рекомендованные Делойтом бизнесу для преодоления неопределенности в будущем, могут стать частью этих мер.

Список литературы

1. Framework agreement on Telework, between the ETUC, UNICE/UEAPME and CEEP 2002 // URL http://ec.europa.eu/employment_social/news/2002/oct/teleworking_agreement_en.pdf. (дата обращения: 09.09.2022).

2. Дэлэйт «Юридически значимый электронный документооборот» // URL <https://sscclub.ru/events/deloitte-juridicheski-znachimyj-jelektronnyj-dokumentooborot/>

И. А. Зайцева,

кандидат политических наук, доцент,

Елецкий государственный университет имени И. А. Бунина

ИННОВАЦИОННЫЕ ВОЗМОЖНОСТИ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ФОРМИРОВАНИИ ДОСТУПНОЙ СРЕДЫ ДЛЯ ИНВАЛИДОВ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Аннотация. В статье представлен анализ проблем формирования доступной среды для инвалидов. Особое внимание уделено мерам, которые направлены на создание безбарьерной и доступной среды данной категории населения в рамках государственной социальной политики. Основными направлениями организации доступной среды жизнедеятельности для инвалидов и людей с ограниченными возможностями являются: организация повсеместного доступа инвалидов; доступная среда в образовательных учреждениях; оснащение объектов транспортной и социальной инфраструктур; сопровождение людей с инвалидностью и др. В статье описываются цифровые технологии, вспомогательные устройства, предназначенные для помощи инвалидам.

Ключевые слова: инвалиды, социальная политика, социальная защита, безбарьерная среда, доступная среда, цифровые технологии

DIGITAL INNOVATION IN CREATING AN ACCESSIBLE ENVIRONMENT FOR PEOPLE WITH DISABILITIES: CHALLENGES AND SOLUTIONS IN TODAY'S SOCIETY

Abstract. The article presents an analysis of the problems of creating an accessible environment for people with disabilities. Particular attention is paid to measures aimed at creating a barrier-free and accessible environment for this category of population within the framework of state social policy. The main areas of organizing an accessible living environment for people with disabilities and people with disabilities are: organizing universal access for people with disabilities; an accessible environment in educational institutions; equipping transport and social infrastructure facilities; accompanying people with disabilities, etc. The article describes digital technologies, auxiliary devices designed to help people with disabilities.

Keywords: Disabled people, Social policy, Social protection, Barrier-free environment, Accessible environment, Digital technologies

Выполнение положений Конвенции ООН о правах инвалидов, ратифицированной Россией в 2012 г., актуализировало проблему социальной защиты инвалидов в современном обществе. Предпринимаются усилия по совершенствованию законодательных норм, направленных на улучшение медицинской помощи, расширение условий получения образования, материальной и социальной поддержки инвалидов.

Теоретическую основу данного исследования составили научные труды современных ученых, социологов, политологов, психологов, правоведов, посвященные изучению проблемы социальной защиты инвалидов, а также анализу государственной политики по формированию доступной среды для лиц с ограниченными возможностями здоровья в условиях декларирования модернизационного пути развития и существующих социальных проблем.

Значительный вклад в разработку методических и прикладных аспектов теории стигматизации внесли М. Файн, Е. Гофман и другие; теории дискриминируемого меньшинства внесли С. Бернс, М. Оливер; теории девальвации и валоризации – С. Томас, В. Вольфенсбергер. Вопросы правового регулирования социальной защиты инвалидов нашли отражение в работах И. В. Выдрина, Т. А. Лыхинной и др. Вопросы, связанные с совершенствованием социальной политики России рассматриваются в работах О. А. Колесниковой, Ю. А. Фирсовой и др. Анализ данной литературы позволяет утверждать, что в российской науке сложились научные взгляды, обосновывающие проблематику социальной защиты инвалидов, как одно из важных направлений социальной политики, влияющей на состояние социального роста российского государства в целом и общества, в частности. Одной из актуальных проблем современного общества является формирование доступной среды для инвалидов.

С 2012 г. по 2022 г. количество инвалидов в России уменьшилось. Такие изменения связаны с улучшением качества медицины, условий труда и общего уровня жизни (табл. 1).

Таблица 1

Информация о численности инвалидов по Российской Федерации на 1 января 2022 г. [3].

Численность инвалидов	Из них:							
	мужчины				женщины			
	I группа	II группа	III группа	дети-инвалиды	I группа	II группа	III группа	дети-инвалиды
11 330 574	690 167	1 807 962	2 126 592	420 591	613 887	2 936 409	2 426 569	308 397

Понятие «безбарьерная среда» имеет тесную связь с достойным уровнем жизни. О необходимости создания безбарьерной среды говорится не только в национальном законодательстве, но и в международных документах, например, в Конвенции ООН о правах инвалидов.

В России реализуется государственная программа «Доступная среда», которая нацелена на создание равного доступа людей с ограниченными возможностями к физическому окружению, и ко всем услугам. По поручению Президента РФ В. В. Путина данная программа продлена на период до 2025 г. В 2020 г. в рамках программы предоставлена субсидия 82 субъектам РФ (дооборудовано 8,1 тыс. детских садов; 10,1 тыс. школ, в которых обучаются дети-инвалиды; 66 учреждений адаптивной физической культуры и адаптивного спорта). Утверждено 11 стандартов в области формирования доступной среды с учетом принципа «универсального дизайна». Обучено 1 884 слушателей (курсы повышения по вопросам организации образования обучающихся с ОВЗ и инвалидностью) из 60 субъектов РФ; 320 слушателя (программа «Тифлопедагогика») из 53 субъектов РФ. Осуществлена финансовая поддержка 39 субъектов РФ, реализующих государственные программы по формированию системы комплексной реабилитации. Заключены соглашения с тремя общероссийскими общественными организациями инвалидов (ВОС, ВОИ, ВОГ) [1. С. 9–23].

Активно применяются современные технологии в обеспечении доступной среды. Первое направление – организация скрытого субтитрирования телевизионных программ общероссийских обязательных общедоступных телеканалов. Объем субтитрируемого контента составляет порядка 30 %. В 2020 г. показатель программы по количеству часов произведенных субтитров составил 13 365 часов. Второе направление – выпуск газет, журналов и книг для инвалидов и инвалидов по зрению. На поддержку выпуска периодических изданий в 2020 г. было предусмотрено 48 млн рублей. В 2020 г. было изготовлено 1 779 наименований книжной продукции для слабослышащих и незрячих лиц. Третье направление – доступность для инвалидов сайтов государственных органов. Еще одно направление – доступность портала Госуслуг [1].

В регионах в рамках формирования доступной среды для инвалидов проводится целый ряд мероприятий: мониторинг наличия пандусов в многоквартирных домах, создание безбарьерной среды в медицинских и образовательных учреждениях, торговых центрах; разработаны и внедряются предложения по социализации и трудоустройству инвалидов; создаются условия для занятий спортом и организации досуга.

Активно применяются интерактивные технологии, которые направлены на прямое взаимодействие с человеком. Например, в образовательном процессе активно используется интерактивный стол, который помогает инвалидам научиться работать в группе, получить социальные и когнитивные навыки, развить мелкую моторику рук. Интерактивная стена «Лабрадор» содержит комплект развивающих приложений и игр. Интерактивная стена ПДД позволяет выучить правила дорожного движения в виртуальном режиме, научиться, как действовать в экстренных ситуациях. Интерактивный пол представляет собой напольную проекцию, полностью взаимодействующую с человеком. Эта разработка позволяет очутиться в любой точке мира, не выходя из помещения. Интерактивные технологии позволяют облегчить деятельность человека, позволяют подстроиться под потребности людей с ограниченными возможностями.

Чтобы помочь адаптироваться инвалидам, улучшить их качество жизни используют вспомогательные устройства разного рода. Например, такие вспомогательные технологии для домашних задач и обслуживания, как Google Home или Amazon Echo помогают инвалидам в пользовании компьютером или телефоном, выполняют такие задачи, как, например, назначить встречу, воспроизвести музыку, рассказать о погоде, дать рекомендации по просмотру фильмов, ответить на основные вопросы, задаваемые пользователем в Интернете. Инвалиды могут пользоваться устройствами контроля окружающей среды из категории «Умный дом» (позволяет дистанционно управлять электронными приборами в доме), персональной системой реагирования на чрезвычайные ситуации. Компания eHeart Health Monitoring разработала персональную сигнальную систему, позволяющую отслеживать состояние своего «носителя». Активно применяются роботизированные системы. Ученые из Бристольского университета в Великобритании изготовили с помощью 3D-печати наконечник пальца, предназначенный для использования роботами или в качестве компонента роботизированных протезов (структура имитирует дермальные сосочки, обнаруженные в человеческой коже). Чтобы помочь лицам с рассеянным склерозом, испытывающим трудности при ходьбе, компания Ekso Bionics разработала роботизированный экзоскелетный костюм, обеспечивающего силу и равновесие ног. «ЭкзоАтлет» производит экзоскелеты для реабилитации инвалидов в домашних и клинических условиях. Трость «The Aid» для слепых помогает людям с нарушениями зрения легче передвигаться, в нее встроен GPS-навигатор, который позволяет инвалидам ориентироваться в пространстве. Телефоны с клавишами Брайля, сенсорные смартфоны предназначены для невидящих людей. Компания IrisVision разработала систему визуальной помощи для слабовидящих людей (телефон фиксирует окружающую пользователя сцену с помощью камеры смартфона, а затем перенаправляет изображение в глаза для улучшения ее видимости для слабовидящих людей) [2]. Проект CaterWil производит инвалидные коляски-трансформеры (колесно-гусеничные коляски). Инвалидное кресло Tek RMD позволяет людям с параплегией самостоятельно стоять, облегчает передвижение и совершение ежедневных задач в помещении. Компания «Моторика» производит электромеханические протезы верхних конечностей для детей и взрослых (сменные насадки протезов со стильным дизайном, в протезах используются технологии «умные часы», беспроводной доступ к сети, система снятия электрических импульсов с мышц и др.). MouthStick Stylus – стилус, позволяющий при помощи рта инвалидам самостоятельно пользоваться смартфоном или планшетом. Часы-смартфон Moneual Smart Care предназначены для глухих и слабослышащих, так как реагируют на тревожные звуки вибровывозом и сообщением на дисплее. Компания Community Cars разработало электрокар для инвалидов.

Для определения безбарьерной среды необходимо использовать совокупность объективных показателей и индикаторов. Если значение таких индикаторов низкое, то среда не может считаться доступной. Это, в свою очередь, влечет возникновение у государства соответствующих обязательств. Главный вопрос в определении приоритетов социальной политики в отношении инвалидов – разработка соответствующих социальных стандартов.

Для получения количественных характеристик проблемы осведомленности населения о реализации программы «Доступная среда» по созданной анкете был проведен опрос (выборочная совокупность 200 чел.). Цель опроса: анализ информированности населения о реализации государственной программы «Доступная среда». Распределение опрошенных респондентов по возрастным группам: до 25 лет – 32 %, от 26 до 45 лет – 36 %, свыше 46–32 %. Среди опрошенных – 48 % мужчин к 52 % женщин.

На вопрос «Знаете ли вы о том, что в Липецкой области реализуется государственная программа «Доступная среда?»» 74 % респондентов ответили «да, знаю», 20 % – «нет, не знаю», 6 % – затруднились с ответом. 52 % опрошенных на вопрос «Как вы оцениваете отношение общества к проблемам инвалидов?» ответили «скорее положительное, чем отрицательное», 8 % – «отношение положительное», 22 % – «скорее отрицательное, чем положительное», 12 % – «отрицательное», 6 % – затруднились с ответом. На вопрос «Оцените, в какой мере общество готово к интеграции инвалидов?» 12 % – ответили «полностью готово», 58 % – ответили «скорее готово», 22 % – ответили «скорее не готово», 6 % – ответили «абсолютно не готово», 8 % – затруднились с ответом. 24 % опрошенных убеждены, что социальные объекты в полной мере оборудованы для посещения их инвалидами, 76 % ответили «не в полной мере». Менее доступны для инвалидов транспорт общего пользования и жилые помещения. Ответы на вопрос «Доступны ли объекты социального назначения для инвалидов по вашему месту жительства?» представлены в табл. 2.

Таблица 2

Ответ на вопрос «Доступны ли объекты социального назначения для инвалидов?»

Организации	Да, %	Нет, %
Образовательные учреждения	84	16
Пункты бытовых услуг	68	32
Помещения жилищно-коммунального хозяйства	56	44
Жилые помещения (квартиры, жилые дома)	42	58
Поликлиники, больницы	86	14
Аптеки	82	18
Административные здания органов местной и государственной власти	92	8
Здания медико-социальной экспертизы	86	14
Здания Фонда социального страхования, Пенсионного фонда РФ	88	12
Здания учреждений социального обслуживания	84	16
Почтовые отделения	74	26
Спортивные учреждения	48	52
Магазины, торговые центры	84	16
Организации общественного питания	68	12
Учреждения культуры	72	18
Пешеходные тротуары, переходы	82	18
Места и зоны отдыха	64	36
Транспорт общего пользования	12	88

Таким образом, в России принимаются различные меры по созданию безбарьерной и доступной среды, что дает им возможность получить образование, квалифицированную работу, участвовать в различных сферах жизни общества.

Список литературы

1. Аналитический вестник № 15 (775). Доступная среда: итоги государственной программы за 2020 год и основные мероприятия на 2021 год. Материалы заседания Совета по делам инвалидов при Совете Федерации Федерального Собрания Российской Федерации (Совет Федерации, 6 апреля 2021 г.). Москва, 2021. – 124 с.
2. Вспомогательные цифровые технологии для людей с физическими недостатками и инвалидов. URL: <https://evercare.ru/news/vspomogatelnye-cifrovyte-tekhnologii-dlya-lyudey-s-fizicheskimi-nedostatkami-i-invalidov-chast> (дата обращения: 27.07.2022).
3. Численность детей-инвалидов. URL: <https://sfri.ru/analitika/chislennost/chislennost-detei> (дата обращения: 11.06.2022).

Д. О. Захарова,
студент,

Московский государственный юридический
университет имени О. Е. Кутафина

ПРОБЛЕМЫ ВЕРИФИКАЦИИ С ТОЧКИ ЗРЕНИЯ ЗАКОНА И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Актуальность работы заключается в интенсивности и масштабности использования верификации в связи с информатизацией современного общества. Цель работы – выявление причин и способов незаконного использования личной информации, а также выяснение способов страхования персональных данных с помощью информационной грамотности. Эта работа основана на практической исследовательской деятельности, где основными источниками информации выступили ЕГРЮЛ и документация организаций.

Ключевые слова: верификация, цифровые технологии, цифровая безопасность, аутсорсинговые компании, данные пользователей, конфиденциальность

VERIFICATION PROBLEMS FROM THE POINT OF VIEW OF THE LAW AND INFORMATION SECURITY

Abstract. The relevance of the work lies in the intensity and scale of the use of verification in connection with the informatization of modern society. The purpose of the work is to identify the causes and methods of illegal use of personal information, as well as to find out how to insure personal data with the help of information literacy. This work is completely based on practical research activities, where the main sources of information were the Unified State Register of Legal Entities and documentation of organizations with which the work was carried out.

Keywords: Verification, Digital technologies, Digital security, Outsourcing companies, User data, Privacy

На сегодняшний день верификация – это неотъемлемый атрибут среднестатистического интернет-пользователя, позволяющий идентифицировать личность потенциального пользователя каким-либо информационным продуктом. Но любой продукт развития цифровых технологий влечет за собой полотно неизвестности, из которого злоумышленники большую часть своей жизнедеятельности пытаются взять лоскут личной выгоды, в чем им успешно помогают пробелы в праве, недостатки в механизмах реализации определенных действий. Верификация предполагает передачу личных данных лица другому лицу, чаще всего уполномоченному на это. Передача же личных данных кому-либо уже ведет к наличию конфиденциальной информации одного из акторов данного процесса верификации сразу у двух персон. Что же мы имеем: передача личной информации второму – третьему – любому другому лицу порождает вероятную возможность в дальнейшем использовать эти данные в целях, немного или же совсем кардинально противоречащих желаниям и воле хозяина данной информации. Задача этой работы заключается в выявлении основных пробелов безопасности (если она вообще имеется) верификации, мотивации потенциальных злоумышленников использовать чью-либо информацию, полученную абсолютно законно, незаконно, наиболее важная задача работы – выявить методы наиболее безопасного использования верификации, если уж информационная судьба вдруг столкнет с ней пользователя.

Практически каждый шаг интернет-пользователя сопровождается верификацией: желание создать криптокошелек, водить машину с помощью каршеринговых программ – примеры можно приводить бесконечно. Приложения и программы собирают паспортные данные пользователей, их адреса, фотографии на переднюю камеру и прочую личную информацию, которую пользователь добровольно передает. Стоит выяснить, кто на самом деле собирает информацию о пользователях, кто ее просматривает и в дальнейшем хранит и/или использует. Необходимость верификации пользователя связана с его прямой ответственностью в дальнейшем. Чаще всего данные пользователей, которые проходят верификацию, попадают в аутсорсинговые компании, а не во внутренние подразделения компаний, которые связаны с безопасностью. Проблемы такого распределения данных заключается в следующем: компания, услугами которой пользователь желает воспользоваться, полностью абстрагируется от ответственности за сохранность личных данных пользователей. Почему это происходит?

Чтобы собирать и хранить огромный пласт личных данных пользователя, необходимо иметь штат специально обученных сотрудников, которым необходимо выплачивать заработную плату, обучать их деятельности и оформлять в соответствии с трудовым законодательством Российской Федерации. Гораздо проще передать на проверку личные данные пользователя какой-нибудь небольшой аутсорсинговой компании. Если услуги аутсорсинговой компании представляются более дешевым способом укомплектовки данных пользователей, чем личный штат сотрудников, то, вероятно, существует экономия на каких-то элементах в этой компании: на трудоустройстве работников (их можно официально не устраивать), на офисе (он может попросту отсутствовать, чтобы не тратить корпоративный капитал на аренду). Также можно рассуждать о том, что работники аутсорсинговых компаний получают недостаточно достойную зарплату, чтобы они не пытались получать экономическую выгоду другими способами, о которых мы поговорим позже.

Что же мы имеем в итоге: n-ное количество не трудоустроенных официально людей, получающих небольшую зарплату, работающих с массивом личных данных других людей. Очень большим массивом. Все это потенциально ведет к незаконному использованию личных данных граждан: для незаконного обналичивания денежных средств, для регистрации компаний-однодневок. Перечислять можно бесконечно. Чтобы доказать актуальность аутсорсинговых компаний, мы создали аккаунт в «Делимобиль»: эта организация предоставляет каршеринговые услуги, поэтому запрашивает личные данные пользователя, чтобы в дальнейшем при определенных обстоятельствах он понес ответственность. Для того чтобы успешно создать аккаунт в данном приложении, необходимо в электронном формате подписать (поставить галочку) согласие на обработку персональных данных, где нашего внимания заслуживает пункт 5:

«Передача персональных данных третьим лицам может осуществляться только в случаях, установленных законодательством Российской Федерации, договором с участием Пользователя или с его согласия. Настоящим Согласием я подтверждаю свое согласие на предоставление ООО «Каршеринг Россия» моих персональных данных нижеуказанным партнерам, а также даю согласие на обработку указанными партнерами персональных данных в объемах, способами и на срок, указанных в настоящем согласии, но не более, чем требуется для обеспечения исполнения Договора/договоров аренды ТС»

Данный пункт доказывает гипотезу о передаче личных данных пользователя третьим лицам. В п. 5.7 представляется возможным ознакомиться с данными этой аутсорсинговой компании:

«ООО «Технологии цифровой безопасности» (191014, г. Санкт-Петербург, Басков пер, д. 10, стр. лит. А, оф. 3-Н, ОГРН 1157847309157) – на передачу и поручение обработки персональных данных, указанных в пп. 1.1–1.13 настоящего Согласия, в целях проверки действительности документов и достоверности предоставленной мной информации при прохождении регистрации в Сервисе Оператора».

Следующий шаг – анализ данных этой организации с помощью такого сервиса, как ЕГРЮЛ. Также необходимо выяснить, зарегистрированы ли еще какие-то организации на этот юридический адрес. Оказалось, что еще две компании зарегистрированы в этом же здании, но в разных офисах: ООО «Смарт Дата» (ИНН 7801688920) и ООО «Интеллектуальная безопасность» (ИНН 7816684164).

Для того чтобы обезопасить свои личные данные, граждане Российской Федерации должны внимательно читать документы, напротив которых они отмечают «согласен». В целом аутсорсинговые компании не нарушают законодательства нашей страны: данные пользователей попадают туда абсолютно законно – через подпись, но отследить дальнейший маршрут этих данных невозможно. Последствия передачи личных данных сомнительным лицам весьма печальны: последующая борьба пользователя с незаконно оформленным микрозаймом, юридическая ответственность. Делегирование задач, что происходит, когда, например, «Делимобиль» передает бремя верификации небольшой подозрительной компании, должно сопровождаться появлением определенного рода ответственности: например, «Делимобиль» или любая другая подобная компания будет уведомлять пользователя о том, что ответственность за сохранность его данных – забота той компании, к которой пользователь обратился изначально.

В. В. Зыкова,

магистрант,

Российский государственный университет
нефти и газа имени И. М. Губкина

МЕЖДУНАРОДНАЯ ВАЛЮТА ДЛЯ РАСЧЕТОВ МЕЖДУ ГОСУДАРСТВАМИ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА

Аннотация. Работа посвящена проблеме расчетов между государствами – участниками ШОС в связи со сложившейся в мире ситуации. Ввиду введения санкций против Российской Федерации одной из стран – участниц ШОС и невозможности проводить расчеты в долларах и евро российская сторона вынуждена проводить расчеты в рублях, в том числе и со странами ШОС. В работе исследуется возможность введения в оборот криптовалюты ШОС для произведения международных расчетов, а также способ такого введения: межбанковская биржа.

Ключевые слова: право, цифровые технологии, криптовалюта, межбанковская биржа, ШОС, санкции, международное право

INTERNATIONAL CURRENCY FOR SETTLEMENTS BETWEEN THE SHANGHAI COOPERATION ORGANISATION

Abstract. The article is devoted to the problem of settlements between the SCO member states in connection with the current situation in the world. Due to the imposition of sanctions against the Russian Federation, one of the SCO member states, and the inability to make settlements in dollars and euros, the Russian side is forced to make settlements in rubles, including with the SCO countries. The work examines the possibility of introducing the SCO cryptocurrency into circulation for international settlements, as well as the method of such introduction: Interbank exchange.

Keywords: Law, Digital technologies, Cryptocurrency, Interbank exchange, Sco, Sanctions, International law

Шанхайская организация сотрудничества (далее – ШОС) была создана в 2001 г. для эффективного и более тесного сотрудничества между ее государствами-членами, в том числе в торгово-экономической сфере. На сегодняшний день участниками ШОС являются следующие государства: Индия, Казахстан, Киргизия, Китай, Пакистан, Россия, Таджикистан, Узбекистан. Однако ситуация, возникшая в 2022 г., оказала сильное влияние на торгово-экономическую деятельность ШОС. Российская Федерация (далее – РФ), будучи одним из государств-учредителей, подверглась санкциям со стороны Соединенных Штатов Америки и со стороны Европейского союза (далее – ЕС). Под западные санкции попали активы Центрального банка РФ и золотовалютные резервы. Около \$ 300 млрд резервов было заморожено, что составляет почти половину всех резервов РФ. Российская сторона в свою очередь ввела механизм для обхода западной расчетной инфраструктуры. С 1 апреля 2022 г. в силу вступил Указ Президента «О специальном порядке исполнения иностранными покупателями обязательств перед российскими поставщиками природного газа». РФ установила платеж за газ в рублях, таким образом отказавшись от расчетов в евро и долларах. Такое положение дел не могло не отразиться и на государствах – членах ШОС.

Большинство стран Запада отказались проводить подобные расчеты, тем не менее российская сторона не собирается отступать от принятого решения и продолжает вести расчеты в рублях. И не только в рублях. Российская компания «Газпром» и Китайская национальная нефтегазовая корпорация CNPC в рамках Восточного экономического форума – 2022 договорились о переходе на расчеты в рублях и юанях при поставке газа по газопроводу «Сила Сибири». Алексей Миллер, глава «Газпрома», заметил, что подобный механизм «взаимовыгодное, своевременное, надежное и практичное решение, которое упростит проведение расчетов, станет примером для других компаний и даст дополнительный импульс развитию наших экономик». Стоит отметить, что Китай также подвергается санкциям со стороны западных стран, поэтому уход от расчетов в иностранной валюте будет положительным шагом в сторону укрепления китайской экономики. Подобный механизм расчетов планируется ввести между РФ и Индией: система расчетов в рублях и рупии. В качестве некой точки отсчета в таком механизме предлагают использовать третью валюту – юань. Также проект расчетов в местной валюте рассматривается и в отношении тенге. Россия, Индия, Китай, Казахстан – все эти государства являются участниками ШОС, т. е. тесно взаимодействуют между собой. Учитывая нынешние реалии, государствам – участникам ШОС было бы выгодно выбрать одну валюту для проведения расчетов. Такая валюта не должна быть привязана к долларам и евро ни на материальном, ни на виртуальном уровне. Она должна быть государственной и централизованной. Подобная валюта в истории уже имела место быть.

Похожий опыт был у стран ЕС при введении ЭКЮ – European currency unit в конце XX в.. ЭКЮ представляла собой некую корзину валют для стран-участников ЕВС – европейской валютной системы, которая состояла из определенных сумм валют государств. Количество валют в корзине не было фиксированным и могло быть расширено в случае включения новых государств-членов. Валюта каждой страны-участницы, входившей в систему, имела фиксированный курс по отношению к ЭКЮ, что позволяло формировать устойчивые курсы валют по отношению друг к другу. Кроме того, при использовании ЭКЮ предполагался безналичный расчет. ЭКЮ позволяло уменьшить изменчивость курса и стабилизировать денежно-кредитную систему в ЕС. Странам ШОС следует перенять подобный опыт Европы с учетом прошлых ошибок. Необходимо создать валюту, которая была бы единой для всех стран-участниц ШОС, которая подобна ЭКЮ позволяла бы странам формировать устойчивый курс к этой валюте. При этом следует учитывать, что цифровые технологии сделали большой шаг вперед, поэтому валюта должна выйти на новый технологический уровень.

Для того чтобы реализовать эту идею государства – участники ШОС могут разработать и заключить между собой соглашение о создании межбанковской биржи. В РФ до появления Московской биржи существовала Московская межбанковская валютная биржа. Центральный банк РФ использовал курс, который складывался в результате торгов иностранной валютой, для установления фиксированных и официальных курсов по отношению к иностранным валютам. Такой же механизм можно ввести на уровне экономического пространства ШОС. Межбанковская биржа установит фиксированный и официальный курс уже по отношению к местным валютам. Как было сказано выше, единая валюта должна соответствовать новым технологиям, поэтому вместо валют на биржу будет выставляться криптовалюта, специально разработанная государствами – участниками ШОС. При этом у нее будет

сохранен «золотовалютный стандарт» в отличие от того же доллара. Криптовалюта будет привязана к золоту, драгоценным металлам, нефти и газу, т. е. будет прочно связана с материальными активами. Подобная связь не позволит экономике стран-участниц пошатнуться, так как количество криптовалюты будет ограничено этими материальными активами. Привязка к материальным активам, а не валюте в свою очередь позволит государствам не зависеть от какой-либо иностранной валюты, а полагаться на собственные ресурсы.

Почему стоит использовать криптовалюту в качестве единой валюты? Во-первых, цифровая валюта имеет свой уникальный код, который не поддается подделке. То есть банки государств – членов ШОС смогут заниматься майнингом со своим уникальным кодом, что позволит использовать ее в качестве официального платежного средства, избегая подделок со стороны третьих лиц. Во-вторых, криптовалюта уже сама по себе является валютой, т. е. страны ШОС, в том числе и РФ, смогут значительно уменьшить свою зависимость от расчетов в долларах и евро, сделать свою экономику более независимой. В-третьих, это значительно упростит платежи между государствами, так как криптовалюта будет являться единой валютой, которую страны-участницы смогут обменивать на местную валюту. В-четвертых, как уже говорилось ранее, криптовалюта более технологичное решение, т. к. в ее основе лежит технология блокчейн. Конечно, для простых физических лиц такая система не представляется особо полезной, но для юридических лиц, особенно крупных, например, в нефтегазовой отрасли, это будет удобным механизмом проведения расчетов.

Стоит раскрыть саму сущность криптовалюты. Криптовалюта представляет собой цифровые деньги, в основе которых лежит специальный зашифрованный цифровой программный код. Именно поэтому подделать криптовалюту невозможно, т. к. такой код уникален и не может быть дважды использован. Криптовалюта является децентрализованной валютой, т. е. у нее нет единого центра эмиссии, как у обычных купюр, которые выпускает только Центральный банк. Любой человек при определенных условиях (наличие устройства, электричества, Интернета) может добывать криптовалюту. Количество криптовалют конечно. Так, биткоинов насчитывается в количестве 21 млн. Поэтому добыча бесконечного количества криптовалюты не представляется возможной. Из недостатков можно упомянуть, что, например, курс биткоина находится в постоянных падениях и подъемах от различных ситуаций в мире, даже незначительных. Это результат того, что биткоин не имеет материальной привязки. Но, как говорилось выше, криптовалюта, которая будет производиться межбанковской биржей ШОС будет иметь такую привязку.

Подводя итоги всего вышесказанного, стоит отметить, что в сложившейся в настоящий момент геополитической ситуации в мире странам – участницам ШОС необходимо предпринять действия, направленные на разработку и введения собственной валюты на новом технологическом уровне для проведения расчетов между собой. Для это они на основе опыта европейских стран с вводом ЭКЮ могут создать собственную цифровую валюту, которую будут реализовывать через межбанковскую биржу, которая будет создана на основе соглашения между странами – участницами ШОС. Это позволит экономике стран не только избавиться от зависимости производить расчеты в валютах других стран, но и стабилизировать собственную экономику. Кроме того, исходя из опыта ЕС, это поможет укрепить отношения между странами-участницами.

Список литературы

1. Бурденко Е. В. Проблемы и история валютной интервенции в Европе в период XIX–XX вв. // Социум: проблемы, анализ, интерпретации: сборник научных трудов. Москва: МПГУ, 2005. С. 274–279.
2. Мелиховский В. М. Криптовалюта: экономические функции и показатели: краткое учебное пособие. Ярославль: Издат. дом ЯГТУ, 2018. 24 с.
3. Семеко Г. В. Суверенная цифровая валюта: новые возможности для трансграничных платежей // Финансовый журнал. 2022. № 4. URL: <https://cyberleninka.ru/article/n/suverennaya-tsifrovaya-valyuta-novye-vozmozhnosti-dlya-transgranichnyh-platezhey> (дата обращения: 12.09.2022).
4. Указ Президента Российской Федерации от 31.03.2022 № 172 «О специальном порядке исполнения иностранными покупателями обязательств перед российскими поставщиками природного газа» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_413296/ (дата обращения: 10.09.2022).
5. Andre Louw The ECU: Facts and Prospects. 2017. June. URL: <https://resume.uni.lu/story/the-ecu-facts-and-prospects> (дата обращения: 10.09.2022).
6. Andreas M. Antonopoulos Mastering Bitcoin // O'Reilly Media, Inc. 2014. URL: <https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch04.html> (дата обращения: 07.09.2022).

Л. Р. Ибатуллина,
магистрант,

Казанский инновационный университет имени В. Г. Тимирязева

ПРЕДУПРЕЖДЕНИЕ ПРИМЕНЕНИЯ ДОПИНГА, СУБСТАНЦИЙ И МЕТОДОВ, ЗАПРЕЩЕННЫХ ДЛЯ ИСПОЛЬЗОВАНИЯ В СПОРТЕ, С ПОМОЩЬЮ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассматриваются новые профилактические меры предотвращения применения допинга спортсменами, а также субстанций и методов, запрещенных для использования в спорте, с помощью новых цифровых технологий, а также их влияние на минимализацию данных уголовно-правовых проявлений среди участников спортивных соревнований.

Ключевые слова: допинг, спорт, цифровизация, цифровые технологии, нравственные ценности, запрещенные спортивные методы, запрещенные субстанции, уголовное законодательство

PREVENTION OF THE USE OF DOPING, SUBSTANCES AND METHODS PROHIBITED FOR USE IN SPORTS USING DIGITAL TECHNOLOGIES

Abstract. The article discusses new preventive measures to prevent the use of doping by athletes, as well as substances and methods prohibited for use in sports with the help of new digital technologies, as well as their impact on minimizing these criminal manifestations among participants of sports competitions.

Keywords: Doping, Sports, Digitalization, Digital technologies, Moral values, Prohibited sports methods, Prohibited substances, Criminal legislation

Существование в настоящее время единого свода правил на международном уровне – Всемирного антидопингового кодекса – является главным достижением в сфере предупреждения применения субстанций и методов, запрещенных в спорте. Стоит объективно признать, что эффективная профилактическая работа против применения допинга непосредственным образом связана с международным сотрудничеством всех стран [1. С. 126].

Для эффективной профилактики допинговых нарушений необходимо не только строгое карательное регулирование, но и использование современных технологических решений для успешного контроля и надзора за спортсменами.

В настоящее время стоит отметить, что существует меры, которые осуществляют контроль касаясь применения спортсменами запрещенных субстанций, речь идет про систему ADAMS (Anti-Doping Administration & Management System). Данная система представляет собой программу, которая хранит данные о спортсменах.

Каждый спортсмен обязан быть зарегистрирован в данной системе, она содержит в себе информацию о местонахождении спортсмена, о пройденных допинг-тестах, результатах допинг-тестов, о наличии разрешения на использование запрещенных субстанций в терапевтических целях. На сайте РУСАДА есть возможность проверить любой препарат на наличие в нем субстанций, которые запрещены для использования в спорте [2. С. 36].

Также существует мобильное приложение «Антидопинг ПРО», которое также выполняет аналогичную функцию. Наличие такой возможности позволит спортсмену самостоятельно осуществлять контроль над тем, что он сам употребляет. Успех профилактики непосредственно связан с профилактической работой с самим спортсменом.

Разработка образовательных профилактических мер началась с 2015 г., когда ВАДА разработала систему электронного обучения «Спортивная обучающая программа о здоровье и антидопинге» (ALPHA), такая программа находилась в Интернете [3. С. 103].

Далее, в 2018 г. ВАДА запускает новую образовательно-электронную платформу, которая носит название «Антидопинговое обучение» (ADeL). Данная платформа по своей сути представляет собой более усовершенствованную систему ALPHA, которая существует в более масштабном размере. Данная платформа также обеспечивает доступ ко всем образовательным блокам, которые существовали в системе ALPHA, все эти правила непосредственно связаны с антидопинговыми правилами и этическими нормами.

Так, стоит отметить, что в 2019 г. ВАДА запустило мобильное приложение, которое отслеживает информацию о местонахождении спортсмена – Athlete Central. Здесь стоит отметить, что правила о местонахождении спортсмена являются одним из важных компонентов программы внесоревновательного антидопингового тестирования.

То есть существует правило касаясь того, что ограниченное количество спортсменов высшего уровня в зарегистрированном пуле тестирования обязано предоставлять антидопинговой организации информацию, где их можно найти в течение одного часа каждый день.

Таким образом, отметим, что использование современных технологических решений для успешного контроля и надзора за спортсменами – современных digital-технологий – способно в превентивном порядке существенно уменьшить количество преступлений и правонарушений, коррелирующих с нарушением антидопинговых правил.

Список литературы

1. Беляев В. А. Профилактические меры борьбы с допингом // Актуальные проблемы гуманитарных и естественных наук. – 2018. – № 7. – С. 126.
2. Осипова И. С. Педагогическая профилактика нарушений антидопинговых правил юными спортсменами // Инновационные технологии в физическом воспитании, спорте, физической реабилитации. – 2018. – № 1. – С. 36.
3. Митин Е. А. Профилактика применения допинга в спорте // Наука в современном обществе. – 2018. – № 2. – С. 103.

О. П. Ильина,

кандидат экономических наук, профессор,
Санкт-Петербургский государственный экономический университет

АРХИТЕКТУРА ПРЕДПРИЯТИЯ КАК ИНСТРУМЕНТ РЕГУЛИРОВАНИЯ ПРОЕКТА ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. Цифровая трансформация – проект, нацеленный на изменение бизнес-системы, организационной, процессной и функциональной систем управления предприятием, ИТ-системы, обеспечивающих эффективное применение цифровых технологий. Проект цифровой трансформации включает работы, согласованные с архитектурой цифрового предприятия, в которой отражены как бизнес-инновации, так и решения в сфере информационных систем и цифровых технологий. Для управления проектом цифровой трансформации можно воспользоваться интегральным показателем «цифровая зрелость архитектуры предприятия», который отражает динамику цифровой трансформации и достигнутые результаты.

Ключевые слова: цифровые технологии, архитектура предприятия, цифровая трансформация, уровень зрелости, бизнес-архитектура, архитектура данных, архитектура приложений, архитектура ИТ-инфраструктуры

THE ENTERPRISE ARCHITECTURE AS A TOOL FOR LEGAL REGULATION OF THE DIGITAL TRANSFORMATION PROJECT

Abstract. Digital transformation is a project aimed at changing the business system, organizational, process and functional enterprise management systems, IT systems that ensure the effective use of digital technologies. The digital transformation project includes activities aligned with the digital enterprise architecture, which reflects both business innovations and solutions in the field of information systems and digital technologies. To manage a digital transformation project, you can use the integrated indicator “digital maturity of the enterprise architecture”, which reflects the dynamics of digital transformation and the results achieved.

Keywords: Digital technologies, Enterprise architecture, Digital transformation, Maturity level, Business architecture, Data architecture, Application architecture, IT infrastructure architecture

Цифровая трансформация экономики РФ – национальная цель развития страны на период до 2030 г. Проект цифровой трансформации осуществляется на основе четырех показателей:

- достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы;
- увеличение до 95 % доли массовых социально значимых услуг, доступных в электронном виде;
- рост до 97 % доли домохозяйств, которым обеспечена возможность широкополосного доступа к Интернету;
- увеличение вложений в отечественные решения в сфере информационных технологий в четыре раза по сравнению с показателем 2019 г.

Для предприятий в эпоху цифровой трансформации требуется объективная оценка уровня цифровой зрелости – на начальном и конечном этапах проекта. Для этой цели целесообразно применить оценку цифровой зрелости архитектуры предприятия, которая характеризует содержание и взаимосвязь бизнес-системы и ИТ-системы предприятия, ориентированных на достижение стратегических и тактических целей цифровой трансформации. Архитектурные модели предприятия рассматриваются как документ проекта цифровой трансформации, основу для его мониторинга. Согласно общепризнанным стандартам и методологиям [1. С. 3–140], архитектура предприятия включает множество моделей для представления:

- **бизнес-системы** – модели организационной, функциональной, ролевой структуры предприятия, бизнес-процессов, производственных ресурсов (трудовых, материальных, технологического оборудования), продуктов деятельности – продуктов, работ и услуг, связанных цифровых экосистем бизнеса;
- **данных** – модели информационной среды цифрового предприятия, содержащей информационные ресурсы структурированной, полу-структурированной и неструктурированной информации;
- **алгоритмов принятия решений, программ** (приложений) для обработки данных бизнес-функций, поддержки бизнес-процессов, реализации программных и пользовательских интерфейсов для взаимодействия с информационными системами, программами и данными;
- **ИТ-инфраструктуры**, в которой соединены вычислительная система, сетевые коммуникации, системное программное обеспечение, технологическое оборудование. На базе ИТ-инфраструктуры реализуют цифровую платформу для взаимодействия с внешней информационной средой, реализации процессов сбора, передачи, хранения и обработки всех видов данных.

Для построения архитектурных моделей предприятия создана метамодель элементов и язык архитектурного моделирования – Archimate [3]. В моделях архитектуры отражается уровень цифровой зрелости. Проект цифровой трансформации предприятия требует построения различных архитектурных моделей определенного статуса:

AS IS («как есть») – модель архитектуры предприятия базисного уровня, соответствует начальной фазе проекта цифровой трансформации.

TO BE («как будет») – модель целевой архитектуры предприятия, прошедшего цифровую трансформацию.

Migration – модель миграционной архитектуры предприятия на определенном этапе цифровой трансформации.

Цифровая трансформация – эволюционный процесс, в течение длительности проекта возникают изменения работ проекта, архитектурных моделей предприятия. Проект разбивают на ряд этапов, которые характеризуются выполнением комплексов работ проекта, обеспечивающих определенный уровень цифровой трансформации предприятия, устойчивость работы бизнес-системы и ИТ-системы, получение эффектов цифровой трансформации. Эти этапы носят название **PLATEAU** («плато»), для них характерна определенная миграционная архитектурная модель и уровень цифровой зрелости предприятия – **Digital Level (DL)**. В общем случае происходит реализация последовательности этапов PLATEAU:

Plateau 1 -> Plateau 2... -> Plateau n, при этом
AS IS =Plateau 1, TO BE = Plateau n

Преобразование архитектурных моделей:

AS IS -> Mg2 -> ... ->Mg k ...TO BE

В результате цифровой трансформации должен быть обеспечен неуклонный рост цифровой зрелости предприятия:

$DL1 < DL2 < \dots < DLn$

Этап Plateau имеет определенную продолжительность, способность предприятия эффективно работать, обеспечивая получение эффектов цифровой трансформации, выделение таких этапов обусловлено рядом причин:

- отсутствие ресурсов для непрерывного выполнения проектных работ,
- изменения на уровне содержания бизнес-системы, требований к ИТ-системе, круга заинтересованных сторон, возможностей цифровых технологий, инструментальных средств, состав и характеристики ресурсов проекта и т. п.

Уровень цифровой зрелости предприятия основан на оценке архитектурных моделей (табл. 1).

Схема процесса оценки цифровой зрелости предприятия на базе моделей архитектуры предприятия содержит ряд действий:

- создание эталонных архитектурных моделей для оценки цифровой зрелости (табл. 1);
- определение состава компонентов эталонных архитектурных моделей;
- разработка шкал значений атрибутов компонентов эталонных архитектурных моделей (минимальный – максимальный балл);
- градация уровней цифровой зрелости для архитектурных моделей на основании суммы баллов – 0–5 (табл. 2);
- определение требований к компетенциям оценщиков на основе эталонных архитектурных моделей;
- разработка процедуры оценки цифровой зрелости.

Таблица 1

**Состав эталонных архитектурных моделей для оценки зрелости
цифрового предприятия**

Группа	Id	Миним. балл	Максим. балл	Эталонные архитектурные модели
Бизнес-архитектура		1	3	Бизнес-канва (модель А. Остервальдера)
		1	3	Оргструктура предприятия
		1	3	Процессная структура
		1	3	Функциональная система управления предприятием
		1	3	Ролевая структура
		1	3	Мотивационная модель стейкхолдеров
		1	4	Стратегическая модель предприятия
		1	2	Бизнес-сервисы
		1	3	Реестр ресурсов цифрового предприятия
		1	3	Реестр возможностей, компетенций цифрового предприятия
		10	30	ИТОГОВАЯ СУММА по группе 1
Архитектура данных		1	3	Инфоканва предприятия (модель О. П. Ильиной)
		2	3	Архитектура данных – модель «сущность – связь» предметной области (модель Entity «сущность» – Relationship «связь»)
		2	3	Модель информационных потоков (DFD)
		2	3	Реестр документов
		2	3	Макет формы документов
		2	3	Основные данные предприятия (номенклатуры объектов для классификации и кодирования)
		2	3	Структура БД – концептуальная, внешние и внутренняя модели
		2	3	Многомерная структура хранилища данных
		2	3	Модель информационной среды предприятия
	17	27	ИТОГОВАЯ СУММА по группе 2	
Архитектура приложений		1	3	Реестр пользовательских интерфейсов
		1	3	Реестр программных интерфейсов
		1	3	Реестр ИТ-сервисов
		1	3	Модель ИТ-сервисов
		1	3	Модель процессов обработки информации
		1	3	Реестр лицензионного программного обеспечения
		1	3	Реестр облачных сервисов SaS
		1	3	Модель архитектуры программных продуктов
	8	24	ИТОГОВАЯ СУММА по группе 3	
Технологическая архитектура		1	1	Модель узлов вычислительной системы
		1	2	Модель сетевой конфигурации
		1	2	Модель ИТ-инфраструктурных сервисов
		1	2	Реестр ИТ-инфраструктурных сервисов
		1	2	Реестр вычислительных ресурсов
		1	2	Реестр хранимых информационных ресурсов
		1	2	Реестр системного программного обеспечения
		1	2	Реестр технологического оборудования
		1	2	Реестр сенсоров, датчиков и IoT
	1	2	Реестр облачных сервисов IaS	
	10	19	ИТОГОВАЯ СУММА по группе 4	
ИТОГО		45	100	

Таблица 2

Градация уровней цифровой зрелости цифрового предприятия на основе интегральной оценки зрелости архитектурных моделей

Модели	Уровни цифровой зрелости предприятия				
	1-й	2-й	3-й	4-й	5-й
Бизнес-архитектуры	4	10	16	24	30
Данных	7	11	17	22	27
Приложений	3	8	16	20	24
Технологической	3	7	11	16	19
	17	36	60	82	100

Модели архитектуры предприятия оцениваются экспертами, на основании их оценок вычисляется итоговый балл, который соответствует рассматриваемой миграционной модели. По мере перехода в направлении реализации целевой архитектуры цифровой трансформации итоговая оценка уровня зрелости должна пересматриваться. Таким образом, получается измеримая количественная мера цифровой трансформации предприятия, определяемая на основе интегрального показателя архитектурных моделей группой экспертов.

Мониторинг проекта цифровой трансформации должен основываться на анализе значений показателей, их сопоставлении с аналогичными показателями для предыдущего этапа проектных работ, а именно:

1. *Бюджетная стоимость* проекта – рассчитывается на основе плана-графика работ проекта, стоимости назначенных ресурсов, календарей проекта, задач и ресурсов.

2. *Фактические затраты* определяются на основании учетных данных о ходе выполнения работ проекта, использования ресурсов (трудовых и материальных).

3. *Плановый объем* работ рассчитывается в нормо-часах для трудового ресурса по категориям, в единицу времени для оценки достаточности/избыточности ресурсов.

4. *Освоенный объем* на основании учетных данных о ходе работ проекта для трудовых ресурсов, работ и проекта в целом.

5. *Плановая длительность* проекта рассчитывается на основании нормативов времени на выполнение работ проекта.

6. *Фактическая длительность* проекта на основании учетных данных о сроках выполнения работ проекта.

Прогнозные значения показателей:

- бюджетная стоимость для завершения проекта,
- суммарная трудоемкость оставшихся работ,
- срок завершения проекта и др.

Планируемый уровень цифровой зрелости.

Фактический уровень цифровой зрелости.

Оценка цифровой зрелости должна осуществляться синхронно с изменениями, вносимыми в архитектурные модели предприятия. Для этого необходимо наладить информационное обеспечение проекта цифровой трансформации, осуществлять контроль качества данных (актуальности, полноты, достоверно-

сти и точности значений), отражающих изменения в архитектуре предприятия. Основная проблема – поддержать синхронность архитектурных моделей – переход к новой миграционной модели архитектуры предприятия и расчет планируемого уровня цифровой зрелости.

В качестве заключения следует отметить:

Предложенный подход и методика расчета интегрального показателя цифровой зрелости архитектурных моделей предприятия позволяет перейти к количественным измерителям.

Состав моделей архитектуры предприятия каждого вида (бизнес-архитектуры, архитектуры данных, архитектуры приложений и технологической архитектуры) может изменяться по усмотрению экспертов.

Пропорции весовых коэффициентов между группами моделей и внутри групп также могут задаваться по согласованию с экспертами.

Для определенной миграционной архитектурной модели и принятого этапа Plateau следует сохранять значения оценки уровня зрелости для целей анализа.

Можно применять данную методику для задания планируемого уровня цифровой зрелости архитектурных моделей и последующей оценки фактического уровня.

Для проекта цифровой трансформации в разрезе этапов работ учитываются инвестиционные и прочие затраты на достижение очередного этапа Plateau (табл. 3).

Таблица 3

Этапы проекта цифровой трансформации предприятия

Показатели	Этапы проекта цифровой трансформации предприятия					
	Mg1	Mg2			Mg n	ИТОГО
Миграционная модель архитектуры						
Уровень цифровой зрелости	1	2	3		5	
Длительность этапа, дней	5	12			8	
Затраты, тыс. р.	120 000	75 000	20 000		15 000	230 000
Эффекты цифровой трансформации, тыс. р.	0	10 000	50 000		200 000	260 000
Сальдо	-120 000	-65 000	30 000		185 000	30 000

На рис. 1 представлена диаграмма изменения параметров затрат и эффектов цифровой трансформации для условного предприятия.



Рис. 1. Рост уровня цифровой зрелости в процессе цифровой трансформации

Список литературы

1. ArchiMate[®] 3.1 Технические характеристики. URL: <https://pubs.opengroup.org/architecture/archimate3-doc/toc.html> (дата обращения: 06.08.2022).
2. TOGAF 9.2. URL: <https://pubs.opengroup.org/architecture/togaf9-doc/m/mobile-index.html> (дата обращения: 26.08.2022).
3. ГОСТ Р ИСО/МЭК 33004–2017 «Информационные технологии. Оценка процесса. Требования к эталонным моделям процесса, моделям оценки процесса и моделям зрелости».
4. Ильина О. П. Архитектура корпораций и информационных систем: развитие подхода и методологии: учебное пособие. Санкт-Петербург: Изд-во СПбГЭУ, 2021. 152 с.
5. Национальная программа «Цифровая экономика Российской Федерации». URL: <https://digital.ac.gov.ru/> (дата обращения: 26.08.2022).

Г. Т. Касенова,

магистр педагогических наук, учитель истории,
Quantum STEM школа

М. Т. Смаилова,

магистр педагогических наук, учитель математики,
Quantum STEM школа

ВОЗМОЖНОСТИ ПРОЦЕССА ЦИФРОВИЗАЦИИ В СФЕРЕ ОБРАЗОВАНИЯ В КАЗАХСТАНЕ

Аннотация. В данной статье описывается важность процесса цифровизации в сфере образования в Республике Казахстан. Цифровизация – это современный необходимый процесс, характерный для всех сфер жизни общества, и он требует реформирования практически всех сфер, грамотного формирования политики, качественной системы образования и подготовки квалифицированных специалистов. Цифровая эпоха, ставшая современной версией информационных технологий, повысила потребность в совершенствовании системы образования. Образовательная среда XXI в. не только дает качественное, базовое, доступное образование, но и воспитывает учащихся, обладающих новаторскими способностями, критическим отношением, творческим мышлением.

Ключевые слова: образование, цифровые технологии, цифровизация, процесс, требования, развитие, оценка

POSSIBILITIES OF THE DIGITAL PROCESS IN EDUCATION IN KAZAKHSTAN

Abstract. This article describes the importance of the digitalization process in the field of education in the Republic of Kazakhstan. Digitalization is a modern necessary process that is characteristic of all spheres of society, and it requires the reform of almost all areas, the formation of a competent policy, a quality education system and the training

of qualified specialists. The digital age, which has become a modern version of information technology, has increased the need to improve the education system. The modern education system should not only provide quality, basic, affordable education, but also educate students with innovative abilities, a critical attitude, and creative thinking.

Keywords: Education, Digital technologies, Digitalization, Process, Requirements, Development, Assessment

В соответствии с новыми условиями, возникшими в мире, возрастает необходимость заблаговременного изучения моделей, видов и преимуществ гибридного обучения и внедрения его на всех уровнях образовательной системы Республики Казахстан. Это будет способствовать формированию новой системы образования, которая поможет подготовить молодых людей, способных противостоять вызовам цифровой эпохи, хорошо разбирающихся в современных технологиях, знающих разные способы обучения, умеющих преодолевать препятствия в образовании, и способствовать устранению неравенства и пробелов в сфере образования.

Цифровизация – требование времени, соответственно в Республике Казахстан проводится много фундаментальных мероприятий в развитии данной сферы, внедряются государственные программы, одной из которых является программа «Цифровой Казахстан». Нет сомнений, что эта государственная программа окажет большое влияние на развитие в стране цифровых технологий и вхождение в ряды развитых стран. В сентябре 2017 г. данная программа была запущена первым Президентом Республики Казахстан Н. Назарбаевым.

В обращении народу Казахстана в 2017 г. Президент страны выделил важность подготовки образованных кадров, а для этого нужно и важно продумать и рассмотреть систему образования: «Все казахстанцы от студентов до пенсионеров должны снова читать книги и осваивать новые технологии. Вопрос обучения на протяжении всей жизни является нужной частью и нормой» [1].

Необходимость непрерывного образования является основным показателем нашего времени, ведь технологии быстро развиваются и часто устаревают и заменяются новыми. Стремительный прогресс происходит в цифровой сфере. В свою очередь развитие современных технологий, цифровизация образования требуют совершенствования сферы образования.

В наше время множество новых полезных инструментов создают удобства для пользователей – цифровые-учебники, облачная система образования, виртуальные лаборатории, персональный ID для каждого ученика, открытый образовательный контент. Эти инструменты способствуют формированию современного мышления, а также нового типа людей, склонных к освоению этих технологий.

Таким образом, цифровизация – это современный необходимый процесс, характерный для всех сфер жизни общества, и он требует реформирования почти всей деятельности, грамотного формирования политики, качественной сферы образования и подготовки высококвалифицированных специалистов в сфере образования.

В исследовательской работе рассмотрены особенности и возможности применения программы цифровизации в сфере образования в Республике Казахстан.

Актуальность исследования. Цифровая эпоха, ставшая современной версией информационных технологий, повысила потребность в совершенствовании системы образования. Образование XXI в. дает качественное, базовое, доступное образование, но нужно воспитывать учащихся, обладающих новаторскими способностями, критическим отношением, творческим мышлением.

Цель исследования: определить особенности, возможности и перспективы программы цифровизации в Республике Казахстан.

Прогноз исследования: если цифровизация в Казахстане будет включена в образовательную систему, это позволит повысить уровень цифровой грамотности населения и обновить систему образования.

Задачи:

1. Оценка процесса цифровизации в сфере образования в Казахстане.
2. Обзор реализованных мероприятий, проектов и результатов, связанных с процессом оцифровки.
3. Проведение опроса по теме.

Процесс оцифровки является одной из главных особенностей сегодняшнего времени. Можно сказать, что ручной сбор и анализ информации потерял свою актуальность. Большинство развитых стран создали полностью цифровую систему, благодаря которой развивается научно-технический прогресс. Область образования также претерпевает множество изменений вследствие процесса оцифровки. Это связано со стратегией «Казахстан 2030»: 12 декабря 2017 г. Постановлением Правительства РК № 827 согласована государственная реформа «Цифровой Казахстан». Программа будет действовать в период 2018–2022 гг. [2]. В соответствии с ней решается множество задач по развитию сферы образования. Например, актуальным остается вопрос использования сетевых технологий в сфере образования, и в реформе «Цифровой Казахстан» ему уделено большое внимание.

Прежде всего, это подключение образовательных учреждений к высокоскоростному Интернету. Степень охвата учреждений зависит от уровня образования. Согласно данным Национальной базы данных образования, дошкольным учреждениям в 2017 г. были доступны только 54,8 % низкоскоростного Интернета и 29 % высокоскоростного Интернета (рис. 1) [3. С. 1–7].

Из рис. 1 видно, что в 2017 г. по сравнению с 2016 г. доступ к высокоскоростному Интернету (свыше 4 Мбит/с) в общеобразовательных школах увеличился почти вдвое и составил 61,8 %, в средних образовательных заведениях – 72 %. В 2017 г. каждое дошкольное образовательное учреждение было оснащено 2–3 компьютерами, соотношение компьютер: ученик в школах составляло 1:11, в маленьких школах на один компьютер приходилось четыре ученика.

В Казахстане работает единая платформа электронного обучения BILIMLand.kz, появившаяся в 2014 г. Данную программу могут использовать не только школьники и студенты, но и дети дошкольного возраста. Все материалы, необходимые для образовательного процесса, доступны на трех языках. Конечно, электронные методические пособия не могут заменить учителя, однако следует отметить, что их использование значительно повышает качество обучения.



Рис. 1. Показатели регионов, имеющих доступ к широкополосному Интернету

Помимо современного технического оборудования, существует три основных направления оцифровки: для реализации хороших результатов в первом направлении необходим переход на раннее ИКТ-образование и хорошее, современное оборудование. Обе эти меры поэтапно внедряются в стране.

Например, в 2018 г. начало преподавания предмета «Информатика» было изменено: теперь учащиеся изучают основные вопросы информатики с 3-го класса, хотя раньше его начинали осваивать в 5-м. Данное новшество подразумевает обновление содержания учебных программ на основе IT-технологий, 3D-печати, робототехники и современных языков программирования. С учетом таких изменений в учебном плане в 2017 г. курсы повышения квалификации прошли около 5,5 тыс. учителей [3. С. 1–7].

Кроме того, нельзя отрицать, что со временем сроки изучения информатики начнутся с еще более раннего возраста (например, в странах ОЭСР учеников с 1-го класса начинают обучать основам цифровой грамотности). Кроме главного учебного плана, очень часто дети обучаются элективному курсу по робототехнике в студенческих центрах развития науки и других дополнительных учебных заведениях. Большое количество учеников, обучающихся на этих курсах, из Карагандинской области, где в 278 кружках обучается 7 177 детей, и из Павлодарской области, где в 230 кружках получают дополнительные услуги образования 6 916 детей [3. С. 1–7].

Согласно следующему направлению, автоматизация образовательных услуг затронет все уровни образования, от дошкольного до послевузовского. Сегодня в дошкольные образовательные учреждения места распределяются на электронной платформе, а в школах этот вопрос регулируется в трех системах: НБД, электронном журнале (дневнике) и «облачной» бухгалтерии. В сфере технического и профессионального образования до конца 2018 г. планируется оцифровка: конкурсного приема и размещения в общежитии, зачетных книжек, электронных паспортов студентов, расписания занятий и домашних заданий и др. Большая работа делается по третьему направлению, направленному на кадровое повышение качества подготовки специалистов в сфере ИТ-образования. Если посмотреть данные Национального доклада о состоянии и развитии системы образования Республики Казахстан, в 2017 г. в 84 высших учебных заведениях на специальностях ИТ-направлений страны обучалось 24 000 студентов; в 300 среднеобразовательных или профессионально-технических учреждениях – 33 000 студентов [3. С. 1–7].

По распоряжению Правительства на технические специальности выделено дополнительно больше 10 тысяч образовательных грантов. Большое количество студентов, обучающихся на специалистов в сфере цифровых технологий, обусловлено высоким спросом на них. Результаты опроса директоров крупных ИТ-компаний Казахстана в 2017 г. показали, что на рынке недостаточно специалистов в таких областях, как система цифровой политики (64 %), большие данные и аналитика (82 %). Чтобы сбалансировать ситуацию касательно спроса и предложения на рынке труда, в классификацию профессий и специальностей ПОО введены пять новых профессий. Кроме того, новым направлением подготовки отечественных ИТ-кадров является «кибербезопасность», по которой в образовательные программы включены дополнительные предметы.

Резюмируя кратко рассмотренные мероприятия, которые проводились в контексте цифровизации системы образования, можно заметить, что они ориентированы на использование современных технологий, упрощающих и облегчающих основные этапы обучения в образовательной системе. При этом эти процессы должны не только активно внедряться, но и развиваться по мере появления в обществе новых технологических и социальных изменений.

Возможности процесса цифровизации в сфере образования приведены в программе «Цифровой Казахстан», указывающей правильное направление его развития. Эти возможности могут быть реализованы за счет изменений в сфере образования: введения смешанного обучения, который быстро развивается в Казахстане.

В образовании есть различные формы обучения (например, когда ученик или студент учится дистанционно, занимается самообучением или же обучается с учителем). Они помогают рассмотреть время, место, темп и способ изучения материала. При этом необходимо обратить внимание на то, что если от 30 до 79 % учебного времени проводится онлайн, то обучение признается смешанным [4. С. 1–55]. Мы можем определить следующие основные аспекты: индивидуальное обучение, экономия времени на занятиях, вариативная часть системы образования, несинхронность обучения, новые возможности взаимодействия, сокращение связи между учеником и содержанием обучения. Компонентами различных видов обучения являются

обучение в классе, офлайн- и онлайн-обучение. Возможности информационных и коммуникационных технологий способствовали быстрому развитию смешанного обучения, которое оказалось более эффективным, чем обучение полностью онлайн. В частности, специалисты Стэнфордского университета по заказу Федерального департамента образования США изучили более тысячи экспериментальных исследований, сравнивающих обычное, онлайн и другие виды обучения [4. С. 1–55].

Использование принципов смешанного обучения в педагогической практике позволяет учителю достичь следующих целей:

Во-первых, повысить доступность и гибкость обучения, расширить образовательные горизонты обучающихся за счет учета их личных образовательных потребностей, а также темпа и ритма усвоения учебного материала;

Во-вторых, поощрить формирование активной позиции ученика: повысить его мотивацию, самостоятельность, социальную активность, в том числе изучение материала, рефлексию и самоанализ, и, как следствие, повысить значимость образования;

В-третьих, сделать учебный процесс ориентированным на ребенка, т. е. индивидуальным. Если учесть образовательные цели, потребности, интересы и способности, учащийся самостоятельно определяет пути их достижения, а преподаватель выступает в роли помощника и наставника. Изменить стиль и подход работы учителя.

Если начать вопрос смешанного обучения, то в настоящее время нет общепринятой единой их классификации. На сегодняшний день можно выделить два типа: 1) на уровне школьного/вузовского образования, внутри школы/вуза; 2) на уровне индивидуального обучения, которое может быть как основным, так и дополнительным образованием [5]. В классной системе ученик использует такие модели, как работа в группах, в том числе независимых, а на персональном уровне используются модели персонализации обучения: новый профиль, межшкольная группа, индивидуальный учебный план (вуз). Среди этих моделей выделяют: Face-to-FaceDriver («очное обучение»), RotationModel («ротационная модель»), FlexModel («гибкая модель»), OnlineLab («онлайн-лаборатория»), Self-BlendModel («модель «Смешай сам»»), когда студент решает, какой из курсов Brickandmortar следует дополнить дистанционными онлайн-уроками; Online Driver Model («водитель-онлайн-обучение»). ИКТ имеет разные версии. Разнообразие моделей помогает облегчить процессы обучения и для студентов, и для преподавателей.

Казахстан стремится выйти на уровень цифровизации зарубежных стран. Согласно исследованию мирового рынка онлайн-образования и образовательных технологий, проведенному East-West Digital News, заявленный размер рынка составляет примерно 4,5–5,0 трлн долларов США [6. С. 5]. Такие цифры говорят о «тренде» дистанционного образования и в ближайшее время будут только расти.

Казахстан будет использовать денежные средства Всемирного банка для реализации проекта «модернизация среднего образования» в размере 67 млн долларов, значит будет возможность для других проектов [7]. Кроме того, учитываются все аспекты в системе образования, а в будущем они могут быть охвачены современными технологиями и Интернетом.

Как и все новое, смешанное обучение имеет свои плюсы и минусы. Среди преимуществ, как правило, то, что ученик самостоятельно планирует процесс обучения, организует свою деятельность, ориентируясь на конечный результат; принимает определенные решения, определяет объем работ в информационном пространстве, осуществляет поиск и отбор информации, предлагает результаты услуг с использованием информационных технологий. Есть аналогичные преимущества для учителей и лекторов. В частности, один учитель теперь может одновременно обучать многих людей. Кроме того, методы контроля индивидуального планирования личного обучения в современных системах смешанного обучения позволяют учителям задавать вопросы только тем, кто работал самостоятельно. Ведь вопросы часто задают студенты, которые не пытались решить их самостоятельно. Сюда относятся проверочные работы через цифровые ресурсы.

Если даже учитывать много положительных моментов, онлайн- и офлайн-система обучения имеет и свои недостатки. К этому можно отнести грамотность, технологическую зависимость, широкополосный Интернет, стабильность онлайн-режима и безлимитных тарифов, слабый уровень владения технологиями и т. д.

Согласно реформе «Цифровой Казахстан», сегодня всем, в том числе и частному сектору, необходимо активно участвовать в техническом обеспечении всех ступеней системы образования. Только благодаря этому можно совместными усилиями создать образованное и современное общество. Это все расширит горизонты Казахстана в достижении общих целей – войти в число передовых по цифровизации стран мира. Как отметил глава государства, казахстанцы быстро адаптируются и стремятся быть конкурентноспособными [7].

Чтобы доказать нашу точку зрения выше, нами проведен опрос. Был использован метод опроса, так как он позволяет получить доступные и анонимные ответы и подходит для сбора информации об общественном мнении о цифровизации. Так как опрос является количественным методом исследования, он помогает собрать первичную информацию. В качестве преимущества цифровой информации можно отметить, что она понятна каждому. Опрос был создан специально для SurveyMonkey и проведен среди 51 участника, которые дали самые разные ответы. Сделать вывод на основе этих ответов не составило большой проблемы. Прежде всего, были определены возрастные категории участников: 13–39 лет, 20–34 года и 35+. В первой и второй возрастной группе участвовало 43 % корреспондентов, а в третьей – только 14 %, так как тема цифровизации более актуальна среди молодежи.

Для того чтобы узнать, насколько популярна в стране тема цифровизации в стране был задан вопрос № 3, который касался в том числе влияния процесса цифровизации на сектор образования Казахстана. В среднем 32 респондента из 51-го выбрали ответ, что цифровизация затронет и систему образования, в то же время всего семь человек считали, что новая тенденция не затронет систему образования. Иными словами, казахстанцы считают, политика цифровизации оказывает огромное влияние на сферу образования.

После этого необходимо было определить, является ли эффект, упомянутый в предыдущем вопросе, положительным для РК или нет (вопрос № 4). Количество участников, ответивших на этот вопрос, «Оказывает положительное влияние и ведет

к новым возможностям» было больше (33 человека), чем тех, кто придерживался противоположного мнения (18 человек).

Последний вопрос был задан, чтобы определить причину выбора этих вариантов. В этой части ответов подчеркивалось, что цифровизация играет большую роль во всех сферах, и говорилось, что она ведет к культурному, политическому, технологическому и научному развитию.

Если Казахстан хочет выйти на глобальный рынок и соответствовать международным стандартам, то уровень цифровизации в стране должен быть повышен – так звучало большинство ответов. Однако были и такие участники опроса, которые утверждали, что эта тенденция негативно сказывается на трудолюбии, любви к чтению и здоровью молодежи. Кроме того, высказывались мнения, что если за цифровизацией последует автоматизация, то уровень безработицы в стране будет расти.

Вывод. Процесс цифровизации экономики играет важную роль и в системе образования РК, он имеет как свои минусы, так и плюсы. Так, цифровизация, способствуя техническому и научному прогрессу, может разрушать мотивацию к труду у молодых людей. Однако большинство участников готовы к процессу цифровизации и понимают возможности, которые она открывает, в том числе для сферы образования. Вот почему технологии приобретают все большее значение среди рабочих и молодежи. Люди, поддерживающие цифровизацию в сфере образования, четко понимают ее роль в будущем и профессионализации профессии. А отличные от этого мнения могут основываться на отсутствии цифровой грамотности. Отсюда можно сделать вывод, что процесс цифровой трансформации экономики тесно связан с обществом.

Для достижения качественного образования необходимы высокоскоростная сеть «Интернет» и современные технологии. Поскольку качественное образование необходимо для процесса цифровой трансформации общества, требуется введение предмета «Информатика» с 1-го класса в план Министерства РК, активное привлечение детей к робототехнике, создание сети детских технопарков и бизнес-инкубаторов, а также предоставление удаленного доступа к видеоурокам. В рамках цифровизации разработаны и реализованы такие проекты, как национальная образовательная база данных, электронный журнал «Кунделик» и образовательный ресурс Vilimland.kz, электронная очередь в детский сад, онлайн-оформление документов о приеме в образовательные учреждения и др.

Однако у цифровизации есть и слабые стороны. Так, во время пандемии в стране не было возможности обучать всех школьников и студентов онлайн, так как в отдаленных районах и селах интернет-система была слабой. Во многих семьях не было компьютеров, студенты и преподаватели оказались не готовы к внезапным переменам, столкнулись с трудностями. Также создали новые проблемы, такие как стремительное устаревание оборудования, компьютеров и другой техники, заполнение офисов современным оборудованием и возрастающая зависимость от гаджетов.

Процесс цифровой трансформации общества не из легких, но его возможности изучаются, делаются первые шаги в этом направлении. В планах государственного ведомства перевод мировых учебников на русский и казахский языки, а также перевод лекций в электронный формат и проведение интерактивных занятий. По словам

министра образования и науки страны, для того чтобы увидеть результаты работы в школах и детских садах через портал, необходимо вести онлайн-мониторинг со стороны ответственных за образование. Все данные должны быть обобщены в одну базу данных BigData, с помощью которой будет возможен их анализ данных. Онлайн-доступ позволит преподавателям сделать процесс обучения более интересным и стимулирующим, а также задействовать весь потенциал учащихся. Самое главное, будет продолжена работа по развитию цифровой инфраструктуры образовательных организаций. Что касается угроз, то нехватка ИТ-специалистов, риск цифрового неравенства между городской и сельской местностью, снижение потребности в очной форме обучения в связи с учебным планом, нехватка высокопрофессиональных кадров с навыками использования дистанционных технологий, нарушение цифровой безопасности и распространение личной информации может ухудшить качество образования. Кроме того, существует риск потери социальных навыков и негативного влияния на здоровье учащихся.

На основе PEST-анализа были выявлены сильные стороны: начали осваивать продукты Microsoft, в частности Office 365 для образования (куда входят все офисные продукты и Teams). Студенты и преподаватели вуза, административный персонал обучаются тому, как создавать и использовать систему аппаратных совещаний. Появилось много новых возможностей: в университете проводилось систематическое обучение преподавателей: в каждом классе были размещены ноутбук и дополнительный монитор, рядом находились специалисты, которые обучали преподавателей работе с онлайн-инструментами, и как результат – всесторонняя поддержка сектора образования. С экономической точки зрения такая деятельность негативно скажется на государственном бюджете. Дестабилизация отечественного капитала может привести к большим последствиям в будущем, к кризису страны с экономической и политической стороны.

Развитие цифровой среды повысит средний уровень грамотности населения, может наблюдаться прирост квалифицированных специалистов в соответствии с эпохой глобализации. Благодаря чему в стране начнет расти качество и ликвидность местной продукции, и в будущем она сможет сравняться с уровнем мирового рынка. Вновь открываемые корпорации и заводы создают новые рабочие места для людей и способствуют развитию ВВП страны. Однако цифровизация также может изменить ценности людей, например, когда все больше граждан повышают свои ИТ-навыки, они, скорее всего, перейдут в иностранные компании, более привлекательные для профессионалов. В то же время появление новых мировоззрений и ценностей у населения приводит к изменению культуры.

В заключение можно сказать, что процесс цифровой трансформации общества открывает много возможностей для развития образовательного сектора Казахстана. В исследовательской работе оценивалась значимость цифровизации и ее место в системе образования. Ответив на вопросы исследования, цель была достигнута, а гипотеза подтверждена. Из вопросов, открывающих тему, можно сделать следующие выводы.

Среди многочисленных мероприятий, проводимых Казахстаном по модернизации сферы образования, можно назвать масштабный проект «Цифровой Казахстан 2020», благодаря которому выполнены основные цели процесса цифровизации. Например, 451 школа по Казахстану оснащена образовательной системой «Билим

книжка». Кроме того, в настоящее время осуществляется смешанное обучение на платформах Microsoft Teams, Bilimland и Twigbilim. Все это свидетельствует о повышении уровня цифровизации.

В статье описаны возможности цифровизации в сфере обучения посредством смешанного обучения. Смешанное обучение развивает индивидуальные навыки обучения и способствует более тесным отношениям между учащимися и учителями, чем обычная учебная программа. В будущем следует уделять больше внимания обновлению этой сферы, чтобы предвидеть проблемы дистанционного обучения в сфере образования.

Также рассмотрены преимущества и недостатки цифровой системы образования. Если смешанное обучение положительно повлияет на систему самообучения учащегося, в то же время может привести к развитию интернет-зависимости. Учитывая положительные и отрицательные стороны данной образовательной системы, необходимо развивать три основные компетенции, внедряемые Astana IT University в соответствии с современными тенденциями. К ним относятся современные цифровые технологии, базовые профессиональные навыки и личностные качества [8. С. 77]. Таким образом, мы можем четко видеть место процесса цифровой трансформации сферы образования. Для продолжения этого пути развития необходима стабилизация системы общего образования.

Список литературы

1. Государственная программа «Цифровой Казахстан». URL: <https://zerde.gov.kz> (дата обращения: 20.12.2019).
2. Как внедряется цифровизация в казахстанское образование. 16 қараша 2017 ж. URL: <https://strategy2050.kz/ru/news/52316/> (дата обращения: 16.11.2018)
3. Образование и инновации для цифровой трансформации // Стратегия развития Astana IT University 2020–2025 жылдары. – Нұр-Сұлтан, 2020. – С. 1–7.
4. Такижбаева Н. З., Асырбеков Х. Программа «ЦИФРОВОЙ КАЗАХСТАН» и смешанное обучение: взаимосвязь и взаимозависимость // 14 қыркүйек. – 2017. С. 1–55.
5. Сколько денег Минобразования потратило на цифровизацию. 20 қыркүйек 2020. URL: https://ratel.kz/kaz/skolko_deneg_minobrazovanija_potratilo_na_tsifrovizatsiju_proverit_schetnyj_komitet (дата обращения: 20.09.2020).
6. Ефрем А. Цифровизация образования: тренды и перспективы развития отрасли в России и за рубежом // 24 желтоқсан. 2019. С. 5.
7. Цифрлық Қазақстан мемлекеттік бағдарламасы // Қазақстан Республикасының Үкіметі. 20 желтоқсан 2019 ж. URL: <http://adilet.zan.kz/kaz/docs/P1700000827> (дата обращения: 20.12.2019).
8. Молчанова Г. Что такое персонализированное обучение? 20 наурыз. 2020. С. 77.

О. Г. Кирсанова,

кандидат экономических наук, доцент,
Смоленский филиал Финансового университета
при Правительстве Российской Федерации,

Смоленский филиал Саратовской государственной юридической академии

ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В статье анализируются актуальные проблемы правового регулирования персональных данных. Рассмотрены отдельные аспекты защиты персональных данных в условиях цифровизации, уточнены права и обязанности участников правоотношений в рамках регулирования персональных данных и условиях привлечения их к ответственности в случае нарушения требований законодательства. Отдельно рассматриваются правовые аспекты регулирования и защиты биометрических персональных данных, выявлены актуальные проблемы и возможности их решения.

Ключевые слова: право, цифровые технологии, цифровизация, персональные данные, биометрические персональные данные, ответственность, защита

LEGAL ASPECTS OF PERSONAL DATA PROTECTION IN THE CONTEXT OF DIGITALIZATION

Abstract. The article analyzes the current problems of the legal regulation of personal data. Some aspects of personal data protection in the context of digitalization are considered, the rights and obligations of participants in legal relations within the framework of personal data regulation and the conditions for bringing them to responsibility in case of violation of the requirements of legislation are clarified. Legal aspects of regulation and protection of biometric personal data are considered separately, actual problems and possibilities of their solution are revealed.

Keywords: law, digital technologies, digitalization, personal data, biometric personal data, responsibility, protection

Актуальность правового регулирования и защиты персональных данных определена гарантией и защитой одного из базовых конституционных прав человека – права на неприкосновенность частной жизни, что приобретает особую значимость в условиях цифровизации социальных процессов и повышения риска нарушения личного информационного пространства личности, в том числе в корыстных целях, способных составить угрозу жизни и здоровью человека или причинить ему материальный ущерб.

Цифровизация социальных отношений и распространение современных цифровых технологий в практику общественного взаимодействия обусловили необходимость актуализации механизма правового регулирования и защиты персональных данных в условиях роста рисков утраты их конфиденциальности и нарушения права гражданина на неприкосновенность частной жизни.

Зачастую именно персональные данные являются объектом корыстных действий со стороны субъектов правоотношений, использующих их в целях личного обогащения, давления при принятии решений и т.п., что является недопустимым и противоправным в условиях формирования гражданского общества и гарантии конституционных прав человека, защита которых не может быть обеспечена правоохранительными органами вследствие недостаточно развитой правоприменительной практики разрешения правового прецедента, связанного с нарушением права гражданина на приватность его персональных данных.

В Российской Федерации правовое регулирование и защиты персональных данных обеспечено в первую очередь Конституцией Российской Федерации и Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее по тексту – Федеральный закон о защите персональных данных), а также рядом ведомственных нормативных актов.

Редакцией Федерального закона о защите персональных данных от 25.07.2011 № 261-ФЗ было расширено понятие персональных данных, позволившее в свою очередь более четко определить сферу применения норм ст. 2 данного закона, указывающей, что ключевой его целью является обеспечение прав и свобод человека при обработке его персональных данных, включая право на личную и семейную тайну и неприкосновенность частной жизни, что также достаточно тесно связано с нормами ст. 152.2 Гражданского кодекса Российской Федерации (далее – ГК РФ), закрепляющей необходимость охраны частной жизни гражданина.

Вместе с тем, несмотря на исключительную роль Федерального закона о защите персональных данных, сохраняющиеся к настоящему времени проблемы обеспечения неприкосновенности личной и профессиональной информации, обусловлены по-прежнему имеющей место недостаточной проработанностью отдельных аспектов правового регулирования персональных данных [5. С. 34], что обусловило необходимость внесения поправок в Федеральный закон о персональных данных, вступивших в силу 01.09.2022 и направленных на усиление роли государственного контроля в данной сфере и повышение степени защиты персональных данных граждан от противоправного к ним доступа со стороны неограниченного круга третьих лиц.

Основные изменения в Федеральном законе о защите персональных данных, вступившие в силу 01.09.2022, затронули повышение правовой защиты персональных данных, что проявилось в первую очередь в сокращении перечня тех случаев, когда оператор, осуществляющий обработку персональных данных, имеет право не подавать соответствующее уведомление в Роскомнадзор.

Так, из перечня случаев, в отношении которых со стороны операторов не требовалось уведомление Роскомнадзора исключены: персональные данные, обработка которых осуществляется в соответствии с требованиями трудового законодательства; сведения, которые получены оператором в результате заключения договора, одной из сторон которого является субъект персональных данных; сведения, включающие в себя фамилии, имена и отчества; персональные данные, необходимые для оформления однократного пропуска субъекта персональных данных на территорию – место нахождения оператора или иных аналогичных случаях, а также перечень сведений, указанных в ч. 2 ст. 22 Федерального закона о защите персональных данных.

В условиях необходимости соблюдения вступивших в силу поправок оператору до начала обработки персональных данных субъекта необходимо направить уведомление в Роскомнадзор, форма и порядок которых определены письмом Роскомнадзора от 19.08.2022 № 08–75348.

Исключение из данного перечня к настоящему времени составляют случаи обработки оператором персональных данных субъекта, которые включены в государственные информационные системы персональных сведений, созданных для обеспечения информационной безопасности государства и поддержания общественного порядка, а также когда при обработке персональных данных оператором не применяются средства автоматизации, позволяющие размещать персональные данные в информационном пространстве.

Кроме этого, новой редакцией расширяется перечень случаев, на которые особенности обработки персональных данных, разрешенных субъектов для распространения, не распространяются, в частности в соответствии со ст. 10.1 Федерального закона о персональных данных распространение особенностей на обработку персональных данных федеральными и региональными органами исполнительной власти и органами местного самоуправления применяется также в отношении организаций и учреждений, которые находятся в их ведомственном подчинении, что отражено в ч. 15 ст. 10.1 Федерального закона о персональных данных.

Также, согласно редакции Федерального закона о защите персональных данных от 14.07.2022 № 266-ФЗ, операторы, осуществляющие обработку персональных данных, обязаны в случае их утечки, направлять соответствующее уведомление в Роскомнадзор в целях проведения последующего расследования, что, с точки зрения законодателя, позволит повысить степень правовой защиты субъектов персональных данных, с большей эффективностью выявлять и пресекать правонарушения, связанные с использованием персональных данных в мошеннических и иных противоправных действиях.

В частности, в случае выявления факта неправомерной, либо случайной передачи информации, содержащей персональные данные, влекущей нарушение прав субъекта, оператор в течение суток с момента выявления данного инцидента обязан уведомить Роскомнадзор о произошедшей ситуации, ее возможных причинах, характере и степени вреда, который был причинен субъекту данным инцидентом, а также о предпринимаемых в данном случае мерах, направленных на устранение негативных последствий, с указанием сведений о контактном лице. В течение трех суток в Роскомнадзор должны быть предоставлены сведения о результатах проведенного внутреннего расследования и лицах (при наличии), которые виновны в сложившейся ситуации (ч. 3 ст. 21).

В течение десяти рабочих дней с даты получения со стороны субъекта требования о прекращении обработки персональных данных оператор обязан исполнить требование согласно общему правилу посредством прекращения обработки персональных данных, либо обеспечения и контроля прекращения обработки в случае, если по его поручению обработку персональных данных осуществляет обработчик. Исключение составляют случаи, когда обработка персональных данных не требует согласия субъекта. Срок исполнения данного требования может быть продлен опе-

ратором при наличии мотивированного уведомления, направляемого оператором субъекту персональных данных (ч. 5.1 ст. 21).

Также в целях усиления защиты персональных данных законодателем были внесены следующие поправки:

- вводится обязательность взаимодействия операторов, осуществляющих обработку персональных данных, с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) в вопросах информирования о прецедентах, повлекших утрату или неправомерное представление персональных данных субъектов;

- вводятся дополнительные обязанности оператора в части устранения правонарушений, возникших в процессе обработки персональных данных, а также их уточнению, блокированию или уничтожению;

- введены дополнительные требования к оформлению согласия на обработку персональных данных, в частности: до 01.09.2022 согласие должно было быть сознательным, конкретным и информированным, с обозначенного периода требования к нему дополняются предметностью и однозначностью;

- определен перечень требований к содержанию документов, которые определяют политику оператора в части обработки персональных данных, а также требования к содержанию локальных документов в данной сфере.

Также с 01.09.2022 для оператора, осуществляющего сбор персональных данных с помощью информационно-телекоммуникационных сетей, определено, где именно данный оператор обязан опубликовать документ, отражающий его политику в части обработки персональных данных и перечень сведений, которые отражают реализуемые требования и мероприятия по защите персональных данных. В частности, опубликование данных сведений оператором должно быть осуществлено на страницах принадлежащего ему сайта, при помощи которых осуществляется сбор, обработка и хранение персональных данных.

Дополнительно июльской редакцией Федерального закона о защите персональных данных предусмотрено, в частности, распространение действия его отдельных правовых норм за пределами территории Российской Федерации, что повлекло за собой уточнение и дополнение ряда полномочий Роскомнадзора, уточнение обязанностей обработчика персональных данных, осуществляющего их обработку по поручению оператора, в том числе определена степень ответственности иностранного обработчика персональных данных.

Согласно новой редакции Федерального закона о персональных данных, договор, который заключается с субъектом персональных данных, в связи с заключением или исполнением которого обработка персональных данных возможна без согласия субъекта, не может ограничивать или нарушать права и свободы данного субъекта, осуществлять сбор и обработку персональных данных несовершеннолетних, за исключением случаев, которые определены федеральным законодательством, а также исключается бездействие субъекта персональных данных в качестве условия заключения такого договора, что предусмотрено нормами п. 5 ч. 1 ст. 6 Федерального закона о персональных данных. Тем не менее, необходимо принимать во внимание,

что такие условия договора не будут недействительными, однако при их включении в договор обработки персональных данных необходимо получить отдельное письменное согласие субъекта.

Новой редакцией расширены права субъекта персональных данных получение информации от оператора в части обработки его персональных данных, например, запрос информации о способах исполнения оператором обязанностей, которые определены ст. 18.1 Федерального закона о персональных данных (п. 9.1 ч. 7 ст. 14), а также дополнены непосредственные обязанности оператора при сборе персональных данных, в частности:

- обязанность разъяснений субъекту персональных данных правовых последствий его отказа в предоставлении персональных данных, отказа в согласии на их обработку, если такое получение такого согласия является обязательным (ч. 2 ст. 18);
- включение перечня персональных данных, полученных от третьих лиц в отношении субъекта, в перечень тех сведений, которые оператор обязан предоставить субъекту персональных данных до их обработки (п. 2.1 ч. 3 ст. 18).

Срок ответа оператора на запросы Роскомнадзора и субъекта сокращены до десяти рабочих дней с момента получения запроса или обращения (в предыдущей редакции такой срок составлял тридцать календарных дней), тем не менее, допускается, что десятидневный срок может быть продлен на пять рабочих дней, не более, при наличии мотивированного уведомления, которое оператор обязан направить инициатору данного запроса (ч. 1, 2, 4 ст. 20).

Отдельный интерес в условиях цифровизации вызывают аспекты правового регулирования и защиты биометрических персональных данных, в отношении которых в Федеральном законе о защите персональных данных уточнены отдельные положения, касающиеся их обработки.

Согласно ст. 11 Федерального закона о персональных данных, биометрические персональные данные представляют собой сведения, характеризующие биологические и физиологические особенности индивида: анализ ДНК, данные дактилоскопии, рост и вес, радужная оболочка и т.п. Перечень биометрических персональных данных дополнен Постановлением Правительства Российской Федерации от 30.06.2018 № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты правительства Российской Федерации» (далее – Постановление Правительства РФ № 772), согласно которому биометрические персональные данные включают данные изображения лица индивида, которые получены при помощи фото и видеоустройств, а также данные голоса человека, которые получены с помощью звукозаписывающих устройств.

Современное законодательство запрещает оператору осуществлять обработку биометрических персональных данных без письменного согласия субъекта, за исключением случаев, определенных ч. 2 ст. 11 Федерального закона о персональных данных, например, в ситуациях, связанных с отправлением правосудия в части обеспечения национальной безопасности, обороны и противодействия терроризму.

Начиная с 01.07.2018 в Российской Федерации функционирует Единая биометрическая система (далее – ЕБС), оператором которой является ПАО «Ростелеком», представляющая собой цифровую платформу, позволяющую индивиду пройти в удаленном формате идентификацию по биометрическим образцам, необходимую для получения финансовых услуг.

Вступление в силу Федерального закона от 29.10.2020 № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» расширило возможности использования ЕБС в целях получения более полного перечня государственных и финансовых услуг, что позволит, согласно позиции законодательства, посредством формирования коммерческими банками единой биометрической системы повысить степень безопасности финансовых операций и снизить риски совершения мошеннических действий, сформировать более простой протокол идентификации клиентов и оказания услуг. В настоящее время данный вопрос остается открытым.

В августе 2022 г. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Минцифры) уточнило основные принципы работы операторов с биометрическими персональными данными, которые впоследствии будут закреплены в виде правовых норм федерального законодательства о персональных данных, в частности:

- недопустимость сбора биометрических персональных данных без добровольного письменного согласия субъекта.

Сбор биометрических персональных данных возможен посредством мобильного приложения (с 30.09.2022) банка или через банк, в будущем данные полномочия будут предоставлены МФЦ. Сбор биометрических персональных данных из иных источников (например, уличных камер видеонаблюдения) не допускается;

- обязательность загрузки биометрических персональных данных из коммерческих систем в ЕБС, что прямо указано в Федеральном законе от 14.07.2022 № 325-ФЗ «О внесении изменений в статьи 14 и 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации», согласно которому данные, которые загружаются в ЕБС должны быть получены только с согласия человека, при этом уполномоченные банки обязаны уведомить субъекта о правилах хранения информации в ЕБС и порядке ее уничтожения;

- недопустимость смешения биометрических персональных данных, загруженных в ЕБС из нескольких коммерческих систем, актуализация информации в соответствии с установленными стандартами качества и своевременное уничтожение неактуальных или утративших достоверность сведений;

- обеспечение надежного хранения информации в соответствии с требованиями информационной безопасности;

- право, но не обязанность гражданина сдавать биометрические персональные данные, что определяется запретом оператору требования предоставления субъектом биометрических персональных данных и обуславливать отказ в предоставлении услуги их отсутствием (ч. 3 ст. 11 Федерального закона о персональных данных в новой редакции). Исключения составляют случаи, когда обработка биометрических персональных данных не требует согласия субъекта.

Резюмируя изменения законодательства в области защиты персональных данных и биометрических персональных данных, необходимо отметить, что новая редакция Федерального закона о персональных данных направлена на усиление степени их защиты, пресечение по возможности рисков нарушения прав индивида на неприкосновенность частной жизни и ее приватность, а также формирование правовой среды для более эффективного регулирования правовых прецедентов, возникающих вследствие утраты персональных данных клиентов, что в настоящее время является одним из проблемных мест в правоприменительной практике, отражая в большинстве случаев неспособность операторов, Роскомнадзора, сотрудников правоохранительных органов и пр. обеспечить полноценную защиту прав и свобод гражданина в данной области.

Тем не менее, несмотря на ряд позитивных изменений законодательства, по-прежнему имеют место проблемы, связанные с обеспечением защиты персональных данных клиентов, на которые еще в 2018 г. указывала в числе многих В. И. Солдатова, которые, тем не менее, в настоящее время не получили соответствующего правового разрешения.

В первую очередь, в своей научной работе «Защита персональных данных в условиях применения цифровых технологий» автор указывает на недостаточный уровень ответственности субъектов правоотношений в сфере использования персональных данных (операторов, обработчиков и пр.) в случае нарушения законодательства, возникновения инцидентов, повлекших утрату персональных данных субъектов и их неправомерное получение третьими лицами [5. С. 39–40].

Профилактике правонарушений в области обработки персональных данных препятствует небольшая сумма штрафа, максимальный размер которой не превышает 75 000 руб., в то время как, например, согласно Регламенту ЕС 2016/679 от 27.04.2016, GDPR, сумма штрафа за нарушение правил в сфере обработки персональных данных, может достигать до 20 млн евро, что соответствует в условиях актуального курса 1,375 млрд руб. [7].

В данном случае, на наш взгляд, целесообразной является необходимость пересмотра норм Федерального закона о персональных данных и сопряженных норм административного и гражданского законодательства в части усиления мер ответственности в отношении операторов персональных данных, допустивших риски неправомерного использования информации третьими лицами, ее утраты и пр., что в первую очередь должно касаться распространения информации, содержащей персональные данные, с помощью ИТКС Интернет.

Достаточно важным аспектом защиты персональных данных в настоящее время является задача правового регулирования права на персональные данные, размещенные в социальных сетях и мессенджерах (Одноклассники, ВКонтакте, Telegram, Viber, WhatsApp и пр.).

Правовой конфликт заключается в том, что, несмотря на добровольное размещение пользователями персональных данных в сетях при обязательной регистрации, такие данные могут быть использованы третьими лицами в собственных, в большинстве случаев противоправных целях или в коммерческих интересах. Очевидно, что согласие на предоставление информации, которая составляет персональные

данные, третьим лицам, субъекты не дают, что делает незаконной не только деятельность третьих лиц, но также и операторов, и обработчиков персональных данных, допустивших такое получение информации.

Необходимо отметить, что судебная практика по указанной категории достаточно обширна, при этом в качестве истцов могут выступать не только субъекты персональных данных, но также и сами операторы. При этом позиция судов однозначна: персональные данные, содержащиеся в открытых источниках социальных сетей, не являются общедоступными, вследствие чего обязательным является получение согласия субъектов на использование данных третьими лицами в коммерческих или иных целях. Судебные решения позволяют выработать условия, при соблюдении которых персональные данные являются общедоступными: они предоставлены владельцем для доступа широкому кругу лиц. Следовательно, вследствие отсутствия в социальных сетях прямого согласия владельца на предоставление его персональных данных третьим лицам, общедоступными они не являются, следовательно, их использование третьими лицами незаконно и является противоправным деянием.

Ведущий юрист Европейской юридической службы Елена Держиева отмечает, что согласно условиям пользовательского соглашения, которое заключает оператор и владелец персональных данных, последний предоставляет согласие на доступ только к той информации, которую он самостоятельно и добровольно размещает на своей странице социальной сети, но не дает согласия на их обработку третьими лицами [6].

Исключение из данной практики составляет ч. 2 ст. 9 Федерального закона о персональных данных, согласно которой оператор может продолжить их обработку без согласия владельца или в случае его отзыва, если речь касается противодействия терроризму, коррупции или отмыванию доходов, полученных нелегальным путем.

В прочих случаях считаем необходимым дополнить действующее законодательство в сфере защиты персональных данных выработанной судебной позицией и сформировать условия применения норм Закона Российской Федерации «О защите прав потребителей» в целях обеспечения прав граждан на защиту их персональных данных.

Подводя итог, отметим, что безопасность и защита персональных данных и биометрических персональных данных могут быть обеспечены в условиях формирования правовой базы и технических приёмов защиты персональных данных, что особенно актуально в условиях цифровизации большинства социально-экономических процессов.

Кроме этого, должны быть созданы необходимые условия для формирования доказательной базы в решении правовых ситуаций, влекущих за собой необходимость привлечения к ответственности участников отношений, допустивших противоправное поведение, что в настоящее время является одной из слабых сторон правоприменительной практики.

Так, дальнейшее развитие системы правового регулирования и защиты персональных данных в условиях цифровизации социально-экономических процессов, на наш взгляд, должно осуществляться по следующим направлениям:

– формирование и развитие практики проведения независимых исследований в случае выявления факта утечки информации, неправомерного ее получения

третьими лицами, как противовеса расследованиям внутренним, по результатам которых нарушения в большинстве случаев не выявляются;

- разработка и внедрение упрощенного механизма защиты субъектов, чьи права в области защиты персональных данных были нарушены;

- ограничение по времени перехода на следующую страницу пользовательского соглашения, что создаст трудности автоматического проставления маркера согласия и повысит вероятность полного прочтения субъектом текста пользовательского соглашения;

- ограничение на законодательном уровне сроков хранения персональных данных и контроля соблюдения данных сроков и порядка уничтожения и пр.

Другими словами, актуальность решаемой правовой задачи в настоящее время заключается в том, что в условиях развития законодательства о защите персональных данных, необходимо разработать механизм, препятствующий нарушению прав граждан на тайну личной жизни, при этом приоритет данного права гражданина должен быть закреплен на законодательном уровне.

Список литературы

1. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 05.09.2022).

2. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 29.12.2020 № 479-ФЗ // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_372645/ (дата обращения: 10.09.2022).

3. О внесении изменений в статьи 14 и 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации»: Федеральный закон от 14.07.2022 № 325-ФЗ // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_421929/ (дата обращения: 11.09.2022).

4. Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты правительства Российской Федерации: Постановление Правительства РФ от 30.06.2018 № 772 // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_301465/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/ (дата обращения: 06.09.2022).

5. Солдатова В. И. Защита персональных данных в условиях применения цифровых технологий // Lex russica. 2020. Т. 73. № 2. С. 33–43.

6. Являются ли общедоступными персональные данные, размещенные в социальных сетях? URL: <https://www.garant.ru/news/12943:10/> (дата обращения: 12.09.2022).

7. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Электронный ресурс]. URL: <https://eur-lex.europa.eu/> (дата обращения: 11.09.2022).

Е. Ю. Комлев,

кандидат юридических наук,
доцент кафедры муниципального права,
Российский университет дружбы народов;
доцент департамента публичного права,
Национальный исследовательский университет
«Высшая школа экономики»

ЗАСЕДАНИЯ ПРЕДСТАВИТЕЛЬНЫХ ОРГАНОВ МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ В ДИСТАНЦИОННОМ ФОРМАТЕ: ПРАКТИКА И ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Аннотация. В статье исследуется практика проведения заседаний представительных органов муниципальных образований в дистанционном формате. В условиях распространения коронавирусной инфекции проведение заседаний в подобном формате признавалось возможным органами исполнительной власти и судами. В условиях стабилизации эпидемиологической ситуации актуализируется вопрос о нормативном регулировании рассматриваемого вопроса. В работе исследован соответствующий опыт нормативного регулирования в Испании.

Ключевые слова: представительный орган, заседание представительного органа, муниципальное образование, дистанционный формат, местное самоуправление, муниципальная власть, коронавирус

LOCAL COUNCIL SESSIONS IN REMOTE FORMAT: PRACTICE AND PROSPECTS OF LEGAL REGULATION

Abstract. The article examines the practice of local council's sessions in a remote format. In the context of the spread of coronavirus infection, sessions in a such format were recognized as possible by executive authorities and courts. In the conditions of stabilization of the epidemiological situation, the issue of normative regulation of the issue under consideration is being relevant. The paper also studies foreign experience (Spain) of the relevant normative regulation.

Keywords: Local council, Local council's sessions, Municipality, Remote format, Local self-government, Municipal power, Coronavirus

Введение. Распространение коронавирусной инфекции очевидным образом способствовало расширению использования информационно-коммуникационных технологий в различных сферах общественной жизни. Стремительное развитие пандемии привело к логичным для подобного рода нестандартных ситуаций по-

следствиям: нормативное регулирование не успевало за развитием многих правоотношений. Альтернативный взгляд на ситуацию: содержание существующих правовых норм получило в новых условиях расширительное толкование. Вне зависимости от интерпретации произошедших изменений, становится очевидным, что с течением времени возникает потребность в осмыслении произошедших социальных изменений, в том числе с правовой точки зрения.

Одним из таких вопросов, которые требуют осмысления, является возможность проведения заседаний представительных органов муниципальных образований в дистанционном формате. Прежде всего, требует разрешения вопрос о самой возможности такого формата заседаний. Ответ на данный вопрос во многом зависит от контекста (внешних условий).

Основная часть. В непредвиденной ситуации, к которой, несомненно, относится пандемия коронавируса, следует, несомненно, принципиально допускать саму возможность дистанционного формата заседания. Из этого исходит и Министерство юстиции Российской Федерации, в своем письме от 02.02.2021 № 08-9883/21 указавшее на то, что предусмотренная регламентами ряда представительных органов муниципальных образований возможность проведения заседаний в дистанционном формате «в целом не противоречит действующему законодательству» [3].

С таким подходом следует согласиться как минимум в условиях распространения коронавирусной инфекции. Для представительного органа этот вопрос является принципиальным. В самом начале пандемии многие представительные органы проводили заседания в дистанционном формате. Если представить, что такие заседания были бы признаны незаконными (несостоявшимися), это открывало бы дорогу для роспуска таких представительных органов на основании ст. 73 Федерального закона от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» (при условии соблюдения сроков). Такой подход вряд ли соотносится с общими понятиями о справедливости и принципами добросовестности и самостоятельности местного самоуправления.

Схожий подход применяется и в судебной практике. Так, Регламентом совета Элисенваарского сельского поселения Республики Карелия предусмотрена возможность проведения дистанционного заседания совета с использованием различных программ, если они обеспечивают возможность онлайн-общения депутатов и приглашенных лиц и непосредственного (очного) обсуждения вопросов повестки заседания. Лахденпохский районный суд Республики Карелия посчитал (сославшись, среди прочего, на распространение коронавирусной инфекции), что проведение заседания совета при помощи программы skype, не противоречит нормативным актам и является законным (Решение Лахденпохского районного суда Республики Карелия от 14.12.2020 по делу № 2а-330/2020).

В контексте рассматриваемого вопроса представляет интерес определение Седьмого кассационного суда общей юрисдикции от 15.12.2021 № 88а-19751/2021. Такой интерес обусловлен как содержанием судебного акта, так и уровнем его принятия (кассационный суд округа – пока наиболее высокая судебная инстанция среди судов, принимавших решения по подобного рода делам).

В изложенном определении суд признал возможным проведение заседаний в дистанционном формате. При этом дело касалось обжалования ряда положений

Регламента Думы Верещагинского городского округа Пермского, и суд пришел к следующим выводам:

– дистанционный формат участия с применением видео-конференц-связи позволяет депутатам в полном объеме реализовать свои полномочия, связанные с участием в заседании представительного органа: обеспечивает возможность видеть участников заседания, высказать каждому депутату свое мнение по обсуждаемым вопросам и слышать выступления других депутатов. Голосование поднятием рук или карточек позволяет участникам заседания контролировать процесс голосования, правильность подсчета голосов, знать о результатах голосования и принятых Думой решениях, что равносильно присутствию депутата на заседании представительного органа местного самоуправления;

– использование данного способа равносильно присутствию депутата на заседании представительного органа местного самоуправления;

– использование данного технического способа позволяет обеспечить выполнение требования о коллегиальном принятии решений с участием каждого депутата в открытом обсуждении вопросов повестки заседания и условия для беспрепятственного осуществления депутатами своих полномочий;

– суд признал оспариваемые положения Регламента незаконными в связи с тем, что они не соответствуют принципу правовой определенности, в частности: не конкретизируют, что подразумевается под дистанционным участием (по мнению суда, под это определение подходит и участие по почте); недостаточно определенно указывают на основания для проведения заседания в дистанционном формате.

Учитывая большое количество муниципальных образований, варианты отражения соответствующих положений в уставах муниципальных образований (реже) и соответствующих регламентах представительных органов будут изобиловать многообразием, что в целом является нормальным явлением с точки зрения развития местного самоуправления, но может вызвать вопросы с точки зрения ответственности таких положений федеральному законодательству (как в случае с вышеуказанным определением седьмого кассационного суда общей юрисдикции). Во избежание подобных проблем представляется необходимым отразить возможность и условия проведения заседаний представительных органов муниципальных образований в дистанционном формате в федеральном законодательстве.

По такому пути пошли и некоторые зарубежные государства. Так, статья 46 Закона Испании «Об основах местного режима» [2] была дополнена положением о дистанционном формате проведения заседаний местных коллегиальных органов. Согласно данной норме, дистанционный формат возможен в случае наличия исключительных ситуаций (форс-мажора), серьезного коллективного риска, катастроф, препятствующих или несоразмерно препятствующих нормальному функционированию очного режима заседаний коллегиальных органов. При наступлении подобных ситуаций коллегиальный орган, оценив риски и приняв соответствующее решение по согласованию с алькальдом (в муниципиях) или председателем совета (в провинциях), вправе проводить заседания, принимать акты и подписывать соглашения с помощью электронных или телематических средств. Необходимым условием дистанционного участия при этом является нахождение члена коллегиального органа на территории Испании и наличие возможности его идентификации.

Данное положение также указывает, что для этих целей действительными электронными средствами являются аудиоконференции, видеоконференции или другие технологические или аудиовизуальные системы, которые должным образом гарантируют технологическую безопасность, эффективное политическое участие ее членов, действительность обсуждения и голосования по принятым соглашениям.

На примере Испании отметим, что условия проведения заседаний в дистанционном формате сформулированы достаточно определенно, при этом без привязки непосредственно к текущей эпидемиологической ситуации. Такой подход делает рассматриваемую норму универсальной, что предполагает возможность ее применения для иных непредвиденных обстоятельств.

Заключение. В период действия ограничительных мер, связанных с распространением коронавирусной инфекции, можно констатировать, что возможность проведения заседаний представительного органа муниципального образования в дистанционном формате допускалась. По мере развития ситуации и стабилизации эпидемиологической обстановки вопрос о дистанционном формате таких заседаний потребует дополнительной регламентации. Подобная точка зрения находит поддержку в научном сообществе [1. С. 66–70].

Представляется, что принятие нового закона о местном самоуправлении, которое ожидается в ближайшее время в связи с внесением в Государственную Думу соответствующего законопроекта [4], является самым подходящим моментом для регламентации вопроса о дистанционном формате заседаний представительных органов муниципальных образований. На примере зарубежного опыта видно, что нормы подобного характера могут быть универсальны и применимы ко многим непредвиденным ситуациям, без привязки непосредственно к эпидемиологической ситуации. В целом перспективным видится и закрепление условий участия в дистанционном формате, среди которых можно указать наличие возможности идентификации участника, наличие функционирующих видеокамеры и микрофона.

При этом необходимо сохранить как базовое правило проведение заседаний в традиционном формате, а условия проведения дистанционных заседаний (или дистанционного участия отдельных депутатов) должны быть определены с высокой степенью детализации. Природа муниципальной власти предполагает наиболее тесное взаимодействие населения именно с муниципальной властью и именно с депутатами, которых население непосредственно и избирает. Такому взаимодействию способствует личное общение депутатов между собой и депутатов с гражданами (которые также вправе присутствовать на заседаниях).

Список литературы

1. Андреечев И. С. Пандемия COVID-19: практика применения дистанционных форм в парламентских процедурах представительных органов (допустимость и подходы к правовому регулированию) // Конституционное и муниципальное право. 2021. № 9. С. 66–70.
2. О порядке проведения заседания представительного органа муниципального образования: Письмо Минюста России от 02.02.2021 № 08-9883/21 // СПС «КонсультантПлюс».

3. Об общих принципах организации местного самоуправления в единой системе публичной власти: Проект федерального закона № 40361-8. URL: <https://sozd.duma.gov.ru/bill/40361-8> (дата обращения: 28.08.2022).

4. Об основах местного режима: Закон Испании от 02.04.1985 № 7/1985/ Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. URL: <https://www.boe.es/buscar/act.php?id=BOE-A-1985-5392> (дата обращения: 28.08.2022).

Е. Д. Костылева,

кандидат юридических наук, доцент, старший научный сотрудник
направления конституционно-правовых исследований,
Центр исследования проблем правосудия,
Российский государственный университет правосудия

СОЦИАЛЬНЫЕ ГАРАНТИИ РЕАЛИЗАЦИИ ПРАВА НА ОБРАЗОВАНИЕ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассмотрены социальные гарантии права на образование в условиях цифровой модернизации современного образования в России, проанализирован их регулятивный потенциал, формы трансформации в условиях технологизации, раскрыты конституционно-правовые особенности реализации и защиты. Выявлены проблемы реализации социальных гарантий права на образование, влияние современных концепций и принципов развития на содержание и пределы реализации рассматриваемого права в условиях актуализации задач обеспечения жизненно важных интересов человечества. Раскрыты основные направления цифровизации в судах по защите права на образование. Проанализировать правовые вопросы внедрения и использования чат-ботов в практиках защиты.

Ключевые слова: право на образование, социальные гарантии, социальная политика, цифровые технологии

SOCIAL GUARANTEES FOR THE REALIZATION OF THE RIGHT TO EDUCATION IN THE DIGITAL AGE

Abstract. The article examines the social guarantees of the right to education in the conditions of modernization of modern education in Russia, analyzes their regulatory potential, forms of transformation in the conditions of digitalization, reveals the constitutional and legal features of its implementation and protection. The problems of the implementation of social guarantees of the right to education, the influence of modern concepts and principles of development on the content and limits of the implementation of the right in question in the context of the actualization of the tasks of ensuring the vital interests of mankind are revealed. The main directions of digitalization in the courts for the protection of the right to education are revealed. Analyze the legal issues of the introduction and use of chatbots in protection practices.

Keywords: Right to education, Social guarantees, Social policy, Digital technologies

Образованию отведена значительная роль в развитии человеческой цивилизации. Создавая почву для инноваций, оно является системообразующей основой преобразования всех сфер жизнедеятельности человека, поэтому его значение в эпоху цифровых технологий становится приоритетным. Образовательный процесс обусловлен наличием прямых и обратных связей, которые взаимозависимы друг от друга, так как предоставление знаний должно сопровождаться их получением и освоением, иначе сам процесс теряет смысл. Неоспоримое значение в совершенствовании системы образования имеет законодательство, регулирующее реализацию социальных гарантий права на образование.

При цифровой трансформации образование должно сохранять роль регулятора умственных процессов, обеспечивая стабильность деятельности образовательных учреждений.

Социальная политика государства в образовании строится на трех основных принципах: признание важности и необходимости образования; обеспечение права каждого индивида на образование; недопущение в сфере образования дискриминации.

Право на образование – это объективное фундаментальное естественное право, принадлежащее человеку с момента рождения, в то же время его можно рассматривать как субъективное право, гарантированная государством возможность человека пользоваться знаниями с целью повышения своего уровня образования в личных интересах и на благо всего общества. Рассматриваемое право представляет ценность не только для конкретного индивидуума, но и для общества и государства в целом, так как оно заинтересовано в образованных, грамотных гражданах.

Объективность видится и в определении значения других норм права, регулирующих сферу образования. Субъективность – в регулировании разнообразных по своему содержанию общественных отношений, возникающих в системе образования.

В отношении этого права государство выступает как гарант и защитник. Делая вклад в образование населения, расширения его возможностей (имея ввиду внедрение компьютерных технологий) и повышая благосостояние граждан, государство реализует свою социальную функцию. Беря на себя ответственность по реализации права на образование, государство обязано создать и поддерживать такую систему образования, которая позволила бы реализовать данное право в полном объеме на современном этапе цифровой трансформации.

Содержание права на образование имеет сложную правовую конструкцию, включающую в себя несколько взаимосвязанных элементов: общедоступность, получение образования каждым человеком на недискриминационной основе, независимо от возраста; возможность получения неограниченного количества уровней образования в различных формах и организациях; в пределах территориальной доступности; выбор языка обучения и другие.

Для реализации рассматриваемого права необходима определенная социальная инфраструктура, включающая систему образования, состоящую из различных уровней, форм, программ, регламентированных государственными стандартами, дающих полное раскрытие способностей человека во всех сферах жизни.

Международная изоляция и санкции подтолкнули страну к масштабным преобразованиям в образовательной сфере, выходу из Болонского процесса и формированию новой системы образования. Изменения уже коснулись воспитательной работы, исторического просвещения, культурного развития, цифровых технологий в образовании.

Для формирования новой конкурентоспособной, качественной образовательной системы, основанной на современных требованиях, технологизации, прежде всего необходимо разработать правовой механизм реализации свободы и доступности в образовании.

Реализация свободы и доступности в образовании подразумевает равные возможности доступа к качественному образованию, возможности поступления в учебные заведения. Коммерциализация системы образования на всех ступенях, начиная от детского сада, школы, продолжается и в высших учебных заведениях, не позволяя реализовать равный доступ всех слоев населения. В результате страдают наиболее социально уязвимые группы населения: инвалиды, дети из многодетных семей, лица с низкими доходами, мигранты, малочисленные народы. Они уже имеют неодинаковые возможности получения образования на начальном этапе, а в дальнейшем приобретают накопительный характер. Поэтому «доступность образования следует рассматривать не в буквальном смысле, а в социальном – независимо от социального положения» [1. С. 26].

Правовые условия реализации права на образование базируются на основных принципах, таких как равноправие, уважение прав человека, которые воздействуют на содержание законодательных, образовательных норм и являются главными гарантиями их обеспечения.

«Принцип равноправия является одним из главных в системе принципов правового статуса личности и имеет доктринальный характер» [2. С. 78]. Он воздействует на юридическое предназначение права на образование, закрепляя равенство независимо от материального состояния, принадлежности к той или иной социальной группе. Действие принципа направлено на установление равенства в человеческом достоинстве.

Неравенство в образовании порождает социальную дифференциацию на всех уровнях, где есть учебные заведения, предоставляющие платные услуги. Рост социально-экономического неравенства усугубляется действием других факторов расслоения, одним из которых является территориальный (невозможность выбора школы в сельской местности; время на дорогу и т. д.), немаловажное значение имеет социокультурный фактор, потребности получения образования индивидуумом. Действие этих факторов усугубляется доступностью дополнительного образования, современных информационных технологий.

«Принцип уважения прав человека является универсальным, императивным принципом, выступающим критерием почтительного отношения...» [3. С. 54–55]. Реализация права на образование подразумевает уважение личности, прав и свобод человека, признание достоинства, что лежит в основе справедливости и всеобщего уважения. Нарушением принципа уважения считается дискриминация человека в любых проявлениях, умаление достоинства личности, недостойное обращение с иностранцами, рабство, геноцид.

Правовое регулирование образования, как одной из составляющих социальной сферы должно быть обеспечено эффективным механизмом реализации и защиты законодательных норм, гарантирующих осуществление права на образование. Модернизация современного российского общества диктует необходимость пересмотра форм и содержания реализации права на образование, создания более действенного механизма защиты рассматриваемого права.

Одной из основных гарантий реализации права на образование остается судебная защита. Немаловажное значение здесь имеет и право на судебную защиту, включающее «право на обращение в судебный орган, право на квалифицированную юридическую помощь, на законный суд, на рассмотрение дела в разумные сроки, на исполнение судебного акта, на получение компенсации» [4. С. 36–37].

Анализ практики показывает, что нарушение права на образование в основном касается несовершенства законодательства об образовании, и граждане в основном обращаются в Конституционный Суд Российской Федерации о проверке или отмене норм в области регулирования образования.

Жалобы в основном касаются вопросов бесплатности обучения (оплаты второго, третьего высшего образования), свободного выбора языка (к сожалению, реализация данной нормы ограничивается реальными возможностями их практического применения). Встречаются жалобы на общедоступность дошкольного образования, которые в основном связаны с очередями (невключение в очередь лиц, имеющих право, а иногда очередь подходит, когда ребенку уже пора идти в школу, поэтому в очередь становятся фактически с момента рождения ребенка); предоставление места в детском саду без учета места жительства (транспортные неудобства); по поводу оплаты за дошкольное образование. Реализация права на образование не должна зависеть от наличия мест в детских садах, органы местного самоуправления (далее МСУ) в случае нехватки мест обязаны своевременно расширять сеть дошкольных учреждений.

Немаловажное значение имеют споры о предоставлении места в детском дошкольном учреждении по месту жительства и режима посещения (группа полного дня или по присмотру). К сожалению, гарантия приема в ближайший детский сад, в отличие от школы (согласно местожительству), законодательно не закреплена. В крупных городах у родителей есть возможность при записи в очередь отмечать приоритетные детские учреждения, в которые они хотели бы попасть, но у жителей сельской местности такая возможность отсутствует. Заявление о постановке на очередь подается через портал Госуслуг или в МФЦ. Здесь жители сельской местности тоже встречают определенные препятствия (не у всех есть возможность воспользоваться новыми технологиями; территориальная расположенность МФЦ).

Социальная незащищенность в реализации права на образование проявляется и при зачислении в школы (не у всех есть возможность зарегистрировать ребенка на Госуслугах). При регистрации по месту жительства в районе, относящемся к данной школе, ребенок должен быть принят в обязательном порядке (до 30 июня такие дети имеют приоритет), далее школа может принимать всех без ограничения, если есть свободные места. Дети, не зарегистрированные по месту жительства, также имеют право на образование в школьных и дошкольных учреждениях, но для

них существует ограничение – они принимаются после тех, кто имеет регистрацию в данном районе. Но данное ограничение можно рассматривать как дискриминацию и оспорить в суде.

В обязанность органов МСУ входит обеспечение возможности получения образования, реализации права на образование. В их обязанности также входит предварительный учет детей дошкольного возраста и закрепление районов города за образовательными учреждениями с таким учетом, чтобы в школах всем хватало места. В случае отказа в приеме в школу, родителям следует обращаться в органы управления образования (ст. 67 ФЗ № 273).

В современном образовательном законодательстве есть пробелы и противоречия, которые влекут нарушение или ограничение права на образование, не определены конкретные формы и санкции, что затрудняет их защиту судом.

На современном этапе развития информационных технологий особого внимания заслуживает развитие чат-ботов. Их внедрение и использование требуют нормативного закрепления. В настоящее время законодательного закрепления данного понятия нет. Под чат-ботами понимаются «технологии, направленные на понимание языка и генерацию текста». Для работы с типовыми документами чат-боты могут использоваться весьма удачно, но для создания оригинального документа они не подходят, в образовании их использование еще не апробировано.

В период пандемии, когда занятия велись онлайн, не у всех детей была возможность полноценно получать образование. Сейчас, когда расписания занятий, домашние задания, дневники, журналы применяются в электронном формате, возникают проблемы у многодетных семей и малоимущих, сельских школ, которые по экономическим причинам не могут способствовать реализации права на образование. Здесь главная задача государства – организовать конкретную помощь своим гражданам в реализации рассматриваемого права.

Без цифровой коммуникации невозможно в глобальном смысле полностью реализовать право на образование. Ребенок, не имеющий доступа к Интернету, фактически не может принимать участие в образовательном процессе. В сфере обеспечения права на образование в условиях цифровизации государство должно прежде всего гарантировать использование технологий детям из малообеспеченных семей, т. е. обеспечить им гарантированный доступ к информационно-коммуникационным сервисам школ.

Реализация права на образование эволюционирует под воздействием цифровых технологий. Современная реальность требует особого понимания места этого права в постоянно меняющемся цифровом пространстве, полноценного обеспечения их реализации и защиты в информационной сфере. Для этого необходим концептуальный подход, основанный на социальном балансе интересов граждан и государства, только тогда цифровая трансформация будет способствовать обеспечению развитию общества.

Список литературы

1. Костылева Е. Д. Реализация и защита социальных прав и свобод человека в эпоху цифровых технологий // Современный юрист. 2022. № 2 (39). С. 22–31. EDN: PIZBZV

2. Костылева Е. Д. Применение конституционным судом РФ и Европейским судом по правам человека, принципа равноправия при оценке правомерности ограничений конституционных прав и свобод в решениях // Современный юрист. 2020. № 3 (32). С. 77–89. EDN: NQDWIB

3. Костылева Е. Д. Принцип уважения прав человека при оценке правомерности ограничений // Современный юрист. 2020. № 4 (33). С. 53–62. EDN: SLPBLN

4. Умнова-Конюхова И. А., Костылева Е. Д. Судебная защита прав и свобод человека как правовой институт: современное состояние и перспективы развития в Российской Федерации // Социально-политические науки. 2021. Т. EDN: XSUEJN. DOI: 10.33693/2223-0092-2021-11-5-34-40

И. Д. Котилевец,
старший преподаватель,
МИРЭА – Российский технологический университет

ДЕКОМПОЗИЦИОННЫЙ ПОДХОД В ОПРЕДЕЛЕНИИ ТЕМАТИКИ И МЕХАНИЗМА ПРОЕКТНО-ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫПОЛНЕНИИ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

Аннотация. Статья посвящена методологии исследования при подготовке выпускных квалификационных работ, связанных с междисциплинарными темами и участвующих в программе «Стартап как диплом». В статье предложена оптимизация таких работ, значимость для реализации и развития компетенций. Приведены критерии схожести стартапов и выпускных квалификационных работ, что позволяет интерпретировать особенности построения командного взаимодействия в командах стартап-проектов как междисциплинарный подход в рамках программы «Диплом как стартап».

Ключевые слова: выпускная квалификационная работа, дипломное исследование, декомпозиция, декомпозиционный подход, стартап, коллективный проект, цифровизация

DECOMPOSITIONAL APPROACH IN DETERMINING THE SUBJECT AND MECHANISM OF DESIGN AND RESEARCH ACTIVITIES WHEN PERFORMING FINAL QUALIFICATION WORKS

Abstract. The article is devoted to the research methodology in the preparation of final qualification works related to interdisciplinary topics and participating in the program “Startup as a diploma”. The article proposes optimization of such works, significance for the implementation and development of competencies. The criteria for the similarity of startups and final qualification works are given, which makes it possible to interpret the features of building team interaction in startup project teams as an interdisciplinary approach within the framework of the diploma as a startup program.

Keywords: Final qualification work, Diploma research, Decomposition, decomposition approach, Startup, Collective project, Digitisation

С помощью выпускной квалификационной работы (ВКР) студенты любого направления подготовки показывают освоенные теоретические и практические знания и навыки. Однако с учетом скорости цифровизации всех сфер жизнедеятельности человека, в том числе и в образовании, проблема объективности в оценивании конечного уровня обученности выпускников вузов представляет собой проблему при определении меры компетенции будущего специалиста, особенно при проектировании или разработке сложных или масштабных проектов. Дополнительную сложность дают разные типы выпускной квалификационной работы: проектно-аналитическая, которая применяется в естественно-научных, технических и компьютерных направлениях подготовки, и теоретическая, применяемая студентами экономических, гуманитарных, юридических и прочих направлениях подготовки, а также различия в образовательных программах подготовки.

С другой стороны, сам процесс цифровизации различных сфер меняет подход к разработке систем. Сама сложность (в контексте степени трудности для понимания, разработки или верификации) систем, либо применяемого программного обеспечения в абсолютно разных сферах возрастает [1–4]. Это также касается и образовательного процесса, например, компьютерных направлений подготовки, 09.**.** или 10.**.**, так как подобные направления непосредственно связаны со сферой информационных технологий. Усложнение различного рода систем приводят к появлению определенных паттернов для проектирования, моделирования и разработки. В связи с тем, что выпускники нацелены на поиск самых перспективных или оптимальных вариантов решения поставленной проблемы по теме ВКР, увеличивающаяся сложность систем является препятствием для многих студентов, соответственно, это может снизить объективность при оценке работы.

Для нивелирования сложности систем при подготовке к ВКР и сохранении объективности при оценивании конечного уровня студента предлагается использовать различные подходы, методологии проектирования, которые используются при проектировании и разработке сложных информационных систем.

Одним из таких подходов является декомпозиция (рис. 1). По декомпозиции каждая цель делится на задачи, которые разбиваются на подзадачи и так далее, что не противоречит постановке цели и задач при написании ВКР. На рис. 1 показан пример декомпозиционной постановки цели и задач ВКР.

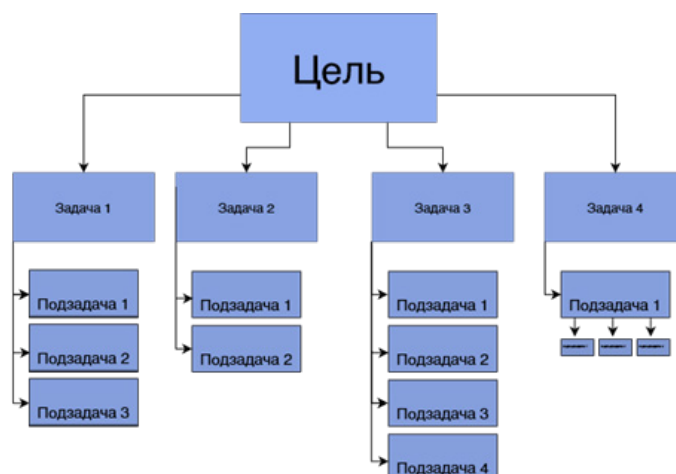


Рис. 1. Пример декомпозиции

Однако при постановке цели и задач в данном случае учитывается, что исполнитель один. Такой подход не всегда возможен при реализации сложных систем, особенно на предприятиях, где, как правило, затронуты команды разработки [5]. Вместо этого, предлагается на основе подхода декомпозиции, который на рис. 1 идет «сверху вниз», от общего к частному, добавить поверх уровня постановки цели еще один уровень, или сверхцель. Сверхцель необходима, с одной стороны, для разработки масштабных систем, достаточно сложных для разработки одним автором, либо для проработки проекта с разных точек зрения, с применением, например, междисциплинарного подхода.

В данном контексте проводится разработка общего проекта коллективом авторов, для каждого из которых, в свою очередь, идет постановка собственных цели и задач, коррелирующих со сверхцелью. Такой подход также применим в рамках программы «Диплом как стартап» [6], где ВКР представляет собой реально существующий бизнес-проект или идею, созданные одним студентом или командой.

В таком случае, каждый задействованный студент в коллективной работе над сверхцелью в рамках своей ВКР будет прорабатывать определенную часть проекта, как модуль единой системы, что, с одной стороны, позволит всем коллективом разработать сложную систему, с другой стороны, совокупное достижение целей ВКР коллективом студентов позволит достичь сверхцель.

В качестве примера в рамках данной статьи приведены две темы ВКР, которые можно разбить как модули единой системы: «Мобильное приложение для реабилитации людей, страдающих когнитивными расстройствами» и «Сбор и анализ психомоторных показателей с помощью мобильного игрового приложения». Темы коррелируют друг с другом и при разработке в качестве единой системы можно добиться определенной синергии модулей-тем ВКР. Примеры целей и задач ВКР в виде декомпозиции показаны на рис. 2 и 3.



Рис. 2. Цель и задача ВКР «Мобильное приложение для реабилитации людей, страдающих когнитивными расстройствами»



Рис. 3. Цель и задача ВКР «Сбор и анализ психомоторных показателей с помощью мобильного игрового приложения»

Как видно из приведенных примеров, работы являются самостоятельными, но их также можно представить как модули единой системы, в данном случае мы можем получить сверхцель (рис. 4). Такой подход, на основе данных примеров, был апробирован в РТУ МИРЭА (ИКБ), обе ВКР получили высший балл на защите выпускных квалификационных работ, проходившей 15.06.2022, а также на основе реализованной системы было получено свидетельство на регистрацию программного обеспечения [7].



Рис. 4. Пример сверхцели для двух ВКР

В дальнейшем можно применять декомпозиционный подход для построения еще более сложных систем, на основе уже реализованной, произвести постановку сверхцели более высокого уровня, где данная разработка, в свою очередь, будет также являться модулем.

Такой подход позволяет студентам разрабатывать качественные выпускные квалификационные работы, которые могут также учитывать потенциальные интересы и потребности работодателей, либо быть целеориентированы на программу «Диплом как стартап».

С учетом особенностей стартапа, а именно того, что это – компания с короткой историей операционной деятельности, то можно выделить несколько схожих критериев ВКР и стартапа, показанных в табл. 1. Стоит отдельно отметить, что критерии и параметры могут варьироваться, в зависимости от сферы применения.

С учетом проведенного анализа, можно наблюдать схожие черты в ВКР и стартапе. Однако один из ключевых критериев ВКР – представление проекта на защите одним разработчиком. С другой стороны, стартап, как правило, представляет собой команду с разделением обязанностей.

Таблица 1

Сравнительный анализ критериев выпускной квалификационной работы и стартапов

Критерии	ВКР	Стартап
Жизненный цикл	1) исследование; 2) сравнительный анализ технологий\продуктов\прочего; 3) постановка требований; 4) проектирование; 5) разработка; 6) апробация	1) поиск идеи; 2) построение бизнес-модели; 3) анализ рынка; 4) поиск финансирования; 5) разработка и тестирование продукта; 6) продвижение продукта; 7) рост
Научно-практическая новизна\ноу-хау\новеллизация	Содержит научную или практическую новизну	Цель – создание инновационного продукта с ориентировкой на практическое применение. Однако в своей основе может содержать научную новизну
Обоснование для разработки	Обоснование представлено в виде актуальности выбранной темы и может содержать сравнительный анализ продуктов\применяемых технологий	Обоснование представлено в виде анализа рынка, которые включает в себя в том числе сравнительный анализ аналогов
Общее число авторов\разработчиков	Пишется и представляется на защите одним автором\разработчиков	Может разрабатываться группой авторов\разработчиков

Наличие апробации\ документов о внедрении\любой другой схожей документации	Необязательно, может иметь заявление\справку о внедрении на предприятие, либо иметь прототип	Должны быть предоставлены документальные доказательства участия в конкурсах или грантах, либо иметь прототип
--	--	--

Декомпозиционный подход при разработке ВКР затрагивает основу системы образования, к разрешению которой призван будущий специалист.

Из-за повсеместной цифровизации ВКР нуждаются в повышении качества содержания и наполнения каждого элемента, усложнении самого проекта, тем самым такой подход позволяет получить в ходе написания ВКР конкурентноспособный проект, а также он легче интегрировать ВКР в программу «Диплом как стартап».

Список литературы

1. Верещагин В. В., Шемякина Т. Ю. Управление рисками в условиях применения технологий информационного моделирования строительных объектов: особенности возможности // Проблемы анализа риска. 2020. № 3. URL: <https://cyberleninka.ru/article/n/upravlenie-riskami-v-usloviyah-primeneniya-tehnologiy-informatsionnogo-modelirovaniya-stroitelnyh-obektov-osobennosti-vozmozhnosti> (дата обращения: 13.07.2022).
2. Горегляд В. П. Цифровой аудит в Банке России как механизм повышения эффективности бизнес-процессов // Государственная служба. 2019. № 1 (117). URL: <https://cyberleninka.ru/article/n/tsifrovoy-audit-v-banke-rossii-kak-mehanizm-povysheniya-effektivnosti-biznes-protsessov> (дата обращения: 16.07.2022).
3. Ешугова С. К., Доргушаова А. К., Чиназирова С. К., Костенко Р. В. Цифровая трансформация банковского сектора // Новые технологии. 2019. № 4. URL: <https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-bankovskogo-sektora-1> (дата обращения: 20.07.2022).
4. Полякова Т. А., Бойченко И. С., Троян Н. А. Информационно-правовые механизмы электронного взаимодействия в сфере правовой информации в условиях цифровизации // Мониторинг правоприменения. 2021. № 1 (38). URL: <https://cyberleninka.ru/article/n/informatsionno-pravovye-mehanizmy-elektronno-go-vzaimodeystviya-v-sfere-pravovoy-informatsii-v-usloviyah-tsifrovizatsii> (дата обращения: 17.07.2022).
5. Тараканов Д. В., Запечалова Л. Ю. Моделирование и реализация командной проектной деятельности в соответствии со стандартами CDIO // ВК. 2022. № 1 (45). URL: <https://cyberleninka.ru/article/n/modelirovanie-i-realizatsiya-komandnoy-proektnoy-deyatelnosti-v-sootvetstvii-so-standartami-cdio> (дата обращения: 17.07.2022).
6. Стартап как диплом. URL: https://minobrnauki.gov.ru/press-center/news/?ELEMENT_ID=25900 (дата обращения: 19.07.2022).
7. Свидетельство о государственной регистрации программы для ЭВМ № 2022660441. URL: https://www.fips.ru/registers-doc-view/fips_servlet?DB=EVM&DocNumber=2022660441&TypeFile=html (дата обращения: 17.07.2022).

В. В. Кудинов,

кандидат педагогических наук, доцент,

Ставропольский филиал

Московского педагогического государственного университета

ПОТЕНЦИАЛ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА С ПРИМЕНЕНИЕМ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ В ОБРАЗОВАНИИ

Аннотация. Конец XX и начало XXI века стали временем одного из самых масштабных технологических прорывов в истории человечества. Он характеризуется как шириной охвата, так и глубиной воздействия на общество, в данный момент речь идет о фундаментальных социальных изменениях. Присутствие цифровых технологий в жизни стало настолько обыденным, что мы с трудом вспоминаем состояние «до» – без текстового процессора, Интернета, навигаторов, компьютерной томографии, банковских карт, электронных баз данных. Следующий этап прогресса – развитие искусственного интеллекта как высший этап развития технологий, сделает присутствие цифровых систем повсеместным и еще более вкрадчивым: транспорт, медицина, образование, – все уже сейчас в значительной степени полагается на цифровые технологии. Активное развитие цифровизации связано с технологиями, основанными на использовании искусственного интеллекта (Artificial Intelligence); внедрение систем электронного обучения в традиционный образовательный процесс приводит к появлению методов, направленных на создание принципиально новой научно-технической продукции. В статье рассматриваются комплексы технологических решений, особенности и методы технологий использования искусственного интеллекта. Анализируются определяющие факторы технологий развития ИИ и те преимущества, которые дает его использование в образовательной среде.

Ключевые слова: образование, цифровые технологии, искусственный интеллект, технологическая сингулярность, программирование, low-code, экзистенция, общество

THE POTENTIAL OF USING ARTIFICIAL INTELLIGENCE USING METHODS OF INTELLIGENT DATA ANALYSIS IN EDUCATION

Abstract. The end of the XX and the beginning of the XXI century became the time of one of the largest technological breakthroughs in the history of mankind. It is characterized by both the breadth of coverage and the depth of impact on society, at the moment we are talking about fundamental social changes. The presence of digital technologies in life has become so commonplace that we hardly remember the state of “before” – without a word processor, the Internet, navigators, computed tomography, bank cards, electronic databases. The next stage of progress – the development of artificial intelligence, as the highest stage of technology development, will make the presence of digital systems ubiquitous and even more insinuating: transport, medicine, education – everything already relies heavily on digital technologies. The active development of digitalization is associated with technologies based

on the use of artificial intelligence (Artificial Intelligence), the introduction of e-learning systems into the traditional educational process leads to the emergence of methods aimed at creating fundamentally new scientific and technical products. The article discusses the complexes of technological solutions, features and methods of technologies for the use of artificial intelligence. The determining factors of AI development technologies and the advantages that its use in the educational environment gives are analyzed.

Keywords: Education, Digital technologies, Artificial intelligence, Technological singularity, Programming, Low-code, Existence, Society

1. Обзор этапов развития, исторический аспект. Текущая технологическая революция началась не вчера. Самый поздний рубеж, который может знаменовать ее старт – это начало 1970-х гг., изобретение микропроцессора (1971 г.) и появление первого рабочего образца персонального компьютера (1973 г.). Вполне возможно, что ее начало можно отнести и к более раннему периоду – например, к событиям 1968 г. (как первому примеру определяющего влияния СМИ на общество), или даже раньше – к деятельности группы дешифровальщиков Алана Тьюринга во время Второй мировой войны, положившей начало всему последующему развитию компьютерной техники. Так или иначе, бесспорно, что к началу XXI в. процесс достиг достаточной степени развития, чтобы начать оказывать непосредственное, зримое и осязаемое влияние на человеческую жизнь. С этого момента можно говорить не только о том, что революция происходит, но и о том, что большинство живущих людей о ней знает и уже сталкивалось с ее плодами. Знаменитый тест Тьюринга признает разумной машину при условии, что в заочном общении человек не сможет отличить ее от другого человека. Такого уровня недавно достиг шахматный компьютер, научившийся не только просчитывать варианты, но и блефовать, то есть учитывать человеческую реакцию противника.

Одним из важнейших аспектов текущей революции является развитие технологии искусственного интеллекта. Разговоры об «искусственном разуме» шли уже давно (как минимум, с момента появления первых компьютеров, а в гипотетическом ключе, в творчестве писателей-фантастов и дальних футурологических прогнозах – и того раньше). Однако пока технологии оставались на уровне все того же компьютера (все равно, централизованного или персонального), «искусственный разум» мог быть лишь фигурой речи, поскольку никакими чертами сознания предполагаемые его образцы на деле не обладали. Первоначальное русское определение – «электронно-вычислительная машина» – было довольно точным (кстати, английский вариант в буквальном переводе означает ровно то же самое, просто звучит красиво и менее понятно).

Компьютер в первоначальном виде – это просто очень мощный и быстрый калькулятор. Он не думает, он производит вычисления. Причем не по своей инициативе, а именно те, которые ему прикажет произвести человек. Позднее к этому добавилась еще роль всесторонней мультимедийной платформы, а также функция хранения и передачи информации (то есть связи с сетью «Интернет»,

универсальной информационной средой). Все это очень ценно само по себе, и отлично укладывается в парадигму компьютера как инструмента для решения всех основных жизненных задач, сформулированную еще Тьюрингом. Это изменило мир, бесспорно, но это далеко не делает компьютер «думающей машиной». Механизмы его расчетов и анализа принципиально отличаются от человеческих мыслительных процессов. К тому же компьютер не обладает совершенно никакой самостоятельностью. По сути, это не новый мозг, это продолжение мозга его создателя (или хозяина), помогающее ему решать определенные задачи, которые иначе были бы ему не по силам. Инструмент, пусть мощный и гибкий, но все равно всего лишь инструмент. Он не думает, он производит вычисления (быстрее, чем человек), хранит информацию (больше, чем человек), и позволяет мгновенно связываться с другими такими же машинами по всему миру (а значит, и с людьми). Говоря об искусственном интеллекте, мы подразумеваем собственно IQ, в то время как эмоциональный интеллект, EQ, остается прерогативой человека, но только активная его составляющая: «машина» не способна испытывать эмоции, но ее можно обучить их распознавать по выражению лица, интонациям, нюансам речи. Распознавать эмоции в каком-то смысле умел даже примитивный детектор лжи. Современные программы распознают сотни нюансов, сравнивая паттерны из базы данных, и оценивают надежность потенциального партнера или клиента.

Философское понимание искусственного интеллекта.

1. Рождение искусственного интеллекта. Настоящей моделью живого мозга с его процессом мышления является не компьютер, а искусственная нейронная сеть (ИНС). Основная стоящая за ней идея – попытаться на аппаратном, электронном уровне воспроизвести работу человеческой, биологической нейронной системы. Для этого живые клетки мозга заменяются процессорами, между которыми выстраиваются связи по образцу биологических нейронных связей. Математически модель была просчитана еще в середине XX в., но тогда уровень развития технологии еще не позволял создать что-то подобное на практике. Это было достигнуто позже. ИНС начали активно воплощаться в жизнь в первые годы XXI в., и дальше развитие шло по пути их усложнения, что выражалось в первую очередь в увеличении количества слоев или уровней нейросети.

Одно из основных и очевидных отличий нейросети от обычного компьютера – нейросети в принципе не программируются. Обратные утверждения часто можно услышать на уровне специальной терминологии – сейчас довольно часто говорят о «программировании нейросетей» как о новой перспективной специальности. Но при этом всегда нужно понимать, что «программирование», которое имеется в виду в таком случае, это не то же самое программирование, о котором говорят применительно к обычным компьютерам. Вместо этого нейросети обучают. Это обучение схоже во многом с обучением биологического организма – в самом базовом виде, «учащемуся» предоставляется информация, на основе которой он делает определенные выводы, которые затем накапливаются, аккумулируются. Данный процесс иногда довольно сложен и по компьютерным меркам небыстр. Усложнение нейросети, увеличение количества ее слоев, еще больше замедляет

процесс. Зато получаемый результат гораздо ближе к реальному человеческому мышлению, как мы его сегодня понимаем (это важная оговорка, потому что работа человеческого мозга и человеческого сознания до сих пор таят в себе немало загадок). Что мы можем сказать точно, так это то, что искусственная нейросеть свободна от тех ограничений, которые на человеческий мозг накладывает биология. ИНС не подвержена старению, а также влиянию других сторонних факторов, которые сказываются на функционировании человеческого мозга – например, заболеваний и травм. Она вообще меньше подвержена воздействию внешней среды (механизм которого в случае с человеком мы даже не всегда полностью понимаем). Это означает, что у искусственного интеллекта гораздо больше времени для обучения, чем у человека. Ему некуда торопиться. А значит, и результатов он может достигнуть несопоставимых – это даже если не учитывать изначально более высокую производительность.

К настоящему моменту наиболее совершенные из нейросетей уже умеют учиться сами. Чего они пока не умеют (и что пока что составляет главное их отличие от человеческого разума) – это самостоятельно ставить себе задачи. Тем не менее на данном этапе мы уже вполне можем говорить об «искусственном интеллекте» (ИИ), чьи принципы работы напоминают человеческие. Пока что он еще ограничен в своих возможностях – ему нужен человек. Никто из специалистов, однако, не сомневается, что рано или поздно будет достигнут и момент самостоятельного целеполагания, и вообще – функциональной независимости искусственного интеллекта от своего создателя.

Различаются только оценки того, как скоро данный момент наступит. По сути, это оценки скорости текущего развития нейросетей, и зависят они во многом от степени информированности и критического настроения оценивающего. Оценки варьируются от 20 лет (звучит, наверное, чаще всего) до 40. Причем произойдет это не обязательно благодаря тому, что «ученые создадут» супер совершенный ИИ (как они создали в свое время, например, атомную бомбу). Весьма вероятно, что имеющиеся нейросети, уже вышедшие, как мы сказали, на уровень самостоятельного обучения, попросту достигнут нового этапа в своем развитии.

2. Технологическая сингулярность. Варьируются и оценки последствий данного события (его часто называют «технологической сингулярностью» – не путать с другими значениями термина «сингулярность», которые встречаются, например, в физике) для человечества. Вызвано это тем, что, как предполагается, превосходство искусственного интеллекта над человеческим в мощности и скорости вычислений и мыслительных процессов столь велико, что функциональная независимость будет означать выход на сцену существа, чьи умственные возможности превосходят человеческие на порядок (как минимум). С этого момента человек перестает быть единственным носителем разума на планете. Более того, он перестает быть на ней «самым умным». Как этим воспользуется искусственный интеллект, осознавший свое превосходство и более не связанный какими-либо объективными ограничениями, мы не знаем. Это закономерно вызывает часто озвучиваемые опасения, что техно-сингулярность грозит человечеству порабощением или вообще геноцидом.

Думается, однако, что данные опасения основаны во многом на непонимании. Человек приписывает ИИ чисто человеческую же мотивацию, и боится ровно того же, чего он опасался бы, если бы это какая-то часть его сородичей вдруг приобрела тотальное интеллектуальное превосходство. В самом деле, у нас нет ровно никаких оснований предполагать в искусственном сознании жажду власти, обиду или страх за собственное выживание – кроме того, что это те самые эмоции, которые, скорее всего, испытывал бы человек, неожиданно осознавший свое превосходство. Но ведь все они, на самом деле, имеют эмоциональную, а не рациональную природу – хотя сам человек и может утверждать обратное ради оправдания своих действий, пытаясь преподнести их как рационально обоснованные. Даже если это сложная эмоция, как жажда власти (растущая, скорее всего, из видоизмененной сексуальности) – это лишь эмоция. То есть именно та сторона сознания, природу и механизм возникновения которой мы пока что не понимаем до конца даже применительно к человеку. Есть серьезные подозрения, что и в человеке эмоции коренятся не в деятельности сознания как таковой, а в биологических и биохимических процессах, протекающих в организме. Если это так, то применительно к искусственному интеллекту (в нынешнем его виде) у нас нет совершенно никаких оснований ожидать появления эмоций, – если мы, конечно, говорим о настоящих эмоциях, а не о симуляции их ради получения желаемой реакции, – но это мотив, связанный с зависимым положением ИИ от человека, а это трудно совместить с понятием техно-сингулярности. С другой стороны, хватает и пессимистических сценариев другого рода, связанных не с какими-либо прямыми действиями искусственного интеллекта, а с общим упадком и вырождением человечества, с утратой им самостоятельности, цели и смысла существования, с превращением его в придаток, зависимое дополнение от «машинного разума», вроде домашних животных [с краткой подборкой сценариев, позитивных и негативных, можно ознакомиться, например, здесь – 4]. В этой связи, однако, вспоминаются апокалиптические прогнозы, которыми сопровождалось почти любое значительное технологическое новшество – будь то железные дороги и поезда или электричество. Тем не менее ИИ уже оказывает значительное влияние на нашу жизнь и будет оказывать еще большее (даже прежде, чем наступит момент техно-сингулярности). Все это влияние можно разделить на два направления. Во-первых, это выполнение ИИ каких-либо действий, то есть прямое участие его в экономике и в жизни человечества вообще [6]. Во-вторых, это само присутствие ИИ в мире и то, каким образом это присутствие способно изменить систему ценностей человека и его взгляды на жизнь, даже без каких-либо активных действий со стороны ИИ. Именно благодаря тому, что искусственный интеллект – не компьютер, способный выполнять (пусть и хорошо) лишь определенный набор функций, предусмотренных его программным кодом, ему могут быть поручены гораздо более сложные и ответственные задания. Ведь он способен к импровизации и даже в определенном смысле – к творческому подходу (пока что – в рамках поставленной перед ним цели). А значит, он способен выполнять те функции, которые обычно возлагаются на человека. Например, управлять транспортным средством в сложной обстановке, или выступать в роли врача, производя диагностику и даже хирургическое вмешательство.

Причем в силу своего огромного превосходства в скорости и производительности с такими задачами он способен справляться значительно лучше человека. Конечно, важный момент здесь – это наличие у искусственного интеллекта таких средств взаимодействия с окружающим миром, которые дадут ему возможность максимально раскрыть свой потенциал (например, развитых сенсорных систем, способных предоставить ему необходимую информацию о происходящем). Это один из важнейших вопросов автоматизации.

3. Искусственный интеллект и человечество. Но, с другой стороны, искусственный интеллект меняет жизнь человека еще до того, как напрямую в нее вмешивается, одним фактом своего существования. Уже сегодня, когда достижение точки бесспорного превосходства является скорее теоретической возможностью (пусть и вероятной), ИИ способен заставить думающего человека по-новому взглянуть на многие привычные понятия. С наступлением техно-сингулярности такая переоценка станет неизбежной для каждого. Важная задача тех, кто уже сейчас предвидит вероятное развитие событий, как раз в том и заключается, чтобы хотя бы отчасти подготовить общественное сознание к неизбежному. Это позволит уменьшить психологический травматизм и быстрее принять новую реальность, кардинально отличающуюся от привычной. Дело в том, что само существование искусственного интеллекта ставит перед человеком ряд интересных (и потенциально, далеко идущих) вопросов. Во-первых, оно означает (как мы уже вскользь упомянули), что человеческий разум больше не является единственным (и даже самым развитым) на планете Земля. А это означает серьезный удар по человеческому самомнению. Для кого-то это существенно. Что даже интереснее, это поднимает ряд неоднозначных вопросов о статусе самого искусственного интеллекта. Что он такое? Можно ли считать его живым? И вот здесь мы неожиданно сталкиваемся с тем, что у нас нет общепризнанного научного определения понятия «жизнь». Точнее, определений существует множество, но ни одно из них не принято научным сообществом как единое или главное, а многие прямо противоречат друг другу. Более того, некоторые часто встречающиеся определения противоречат научно установленным фактам. Например, распространенное определение через способность к размножению не учитывает того, что воспроизводство вообще является распространенным свойством динамических систем, и далеко не только органических. Касательно практически любых признаков, которые используются для определения живого, можно найти подобные примеры, которые отрицают их исключительность и определяющее значение. Мы остаемся с чисто философскими определениями жизни. Уязвимость большей части из них состоит в том, что они так или иначе используют в качестве опоры те же самые научные понятия, в противоречивости которых мы уже убедились. Очевидно, что до тех пор, пока наука не предложит нам более взвешенного и менее спорного определения, на первый план неизбежно выйдут те концепции философов, которые в наименьшей степени к ней апеллируют.

В современной философии наиболее значительными из них, по всей видимости, являются определения жизни через самоосознание, данные философами-экзистенциалистами. Дело в том, что центральным понятием для данного направле-

ния философии является «экзистенция». Буквально это означает «существование», но имеется в виду не одно лишь простое физическое существование. Данную концепцию развивали так или иначе все философы-экзистенциалисты, начиная с Кьеркегора – Ясперс, Хайдеггер, Сартр, Марсель, Камю [например, 10]. До того схожие мысли высказывал, например, Фридрих Ницше, которого сами экзистенциалисты во многом считают своим предшественником. Попадают и версии более раннего происхождения идей – так, истоки экзистенциализма находят в философии эпохи Возрождения (например, у Пикоделла Мирандола), а то и вообще в античности (у того же Платона). Сейчас к идее определения жизни через самоосознание нередко обращаются философы именно в связи с развитием искусственного интеллекта [3]. В общем и целом, если мы отбросим понятное желание «удревнить» свои идеи и посмотрим на их суть, мы придем к тому, что первооснова идей экзистенциалистов – это разделение понятий «существования» и «сущности». Причем существование предшествует сущности и совершенно не обязательно ее влечет за собой. Под «существованием» понимается бытие физическое – то есть то, чем обладают в полной мере и предметы неживой природы. Принципиальное отличие человека заключается именно в понятии «сущности», или экзистенции, если использовать тот термин, который и дал этому течению философии его название.

Что же такое экзистенция? Это, прежде всего, существование индивидуальной уникальности. Кроме того, экзистенция неразрывно связана с сознанием – необходимым условием ее является самоосознание, внутреннее переживание своей сущности. Таким образом, данное понятие в принципе неприменимо к существованию объектов неживой природы. Именно экзистенция и делает человека человеком. То есть для того, чтобы считаться человеком, существо должно, во-первых, существовать физически, но после этого оно еще должно себя осознать как индивида, отделенного от других – обрести экзистенцию.

Нетрудно заметить, что экзистенция не является неизбежным следствием существования – она требует определенного уровня развития сознания. Теоретически мы можем представить себе человека (в физиологическом смысле этого слова, со всеми обычными для человека функциями организма), не обладающего экзистенцией. Правда, в таком случае он принципиально ничем не будет отличаться от животного. Вероятно, в развитии человека был момент, когда он именно это собой и представлял, а человеческая популяция ничем не отличалась от популяции других крупных приматов. В какой момент случился этот переход (обретение экзистенции значимой долей людей как биологического вида) мы сейчас можем лишь гадать – это могло произойти уже с людьми современного вида, или на более ранней ступени эволюции. Последнее вероятно, поскольку неандертальцы (наши «эволюционные кузены», произошедшие от общего с нами предка) демонстрируют черты, наводящие на мысли о возможном достижении экзистенции – погребальные ритуалы, искусство (изобразительное и музыку). Возможно, это связано с достижением определенного уровня развития сознания, что является следствием биологической эволюции центральной нервной системы и идет рука об руку с развитием социума. В таком случае, очень вероятно, что человек современного вида обладал этим свойством либо изначально, либо с очень ранней стадии.

Экзистенция неразрывно связана со взглядом на человека как на объект творчества – прежде всего, собственного. «Человек просто существует, и он не только такой, каким себя представляет, но такой, каким он хочет стать. И поскольку он представляет себя уже после того, как начинает существовать, и проявляет волю уже после того, как начинает существовать, и после этого порыва к существованию, то он есть лишь то, что сам из себя делает» [10. С. 167]. И чуть дальше, еще яснее: «Человек – это прежде всего проект, который переживается субъективно» [10. С. 167]. Иначе говоря, ты – тот, кем ты себя осознаешь. Возможно, из всех существующих сегодня философских понятий – это самое близкое к «жизни», как мы ее понимаем. При этом ключевым фактором для признания экзистенции – то есть жизни – является, так или иначе, наличие сознания. Живым является тот, кто способен осознать себя – свою индивидуальность, свою отдельность от общей массы. Осознать себя как «я». Из этого следует, что если искусственный интеллект, достигший функциональной самостоятельности в точке техно-сингулярности, осознает себя как индивидуально определенное существо, отдельное от своего класса (а в этот момент ему, строго говоря, ничто не мешает это сделать), он обладает экзистенцией, а значит – может (и даже должен) быть признан живым в полном смысле этого слова. В том же, что и человек. А это поднимает еще один интересный вопрос. Искусственный интеллект бесспорно является созданием человека. Если мы признаем его живым, выходит, что человек в принципе способен сотворить новую жизнь. Не передать частичку своей, как происходит при обычном размножении, не сделать слепок или копию, как при клонировании, а создать буквально из ничего, с нуля. Но в традиционных, укоренившихся веками человеческих представлениях это считается прерогативой бога. Собственно, это едва ли не единственная его прерогатива, которая является общей для почти всех современных религий – остальное открыто обсуждениям и трактовкам. Теперь человек вторгается в эту область. Понятно, что с точки зрения науки любые религиозные воззрения остаются в лучшем случае в «серой зоне», где «наука пока не все может объяснить». Тем не менее они являются значимым фактором общественной жизни и распространенной мотивацией поступков многих людей. С практической точки зрения не так важно то, что за этим на самом деле стоит (если стоит), сколько то, что люди об этом думают. Между тем любопытно, что философы-экзистенциалисты успели весьма подробно затронуть и эту тему, хотя конечно, не применительно именно к искусственному интеллекту. Взаимоотношения человека с божественным началом неизбежно были для них одним из ключевых вопросов. Вообще, деление экзистенциалистов на атеистов и религиозных было едва ли не главной их собственной классификацией. Ее предлагал, в частности, тот же Сартр, который относил к экзистенциалистам-атеистам себя самого и Хайдеггера, а к христианским экзистенциалистам – Карла Ясперса и Габриэля Марселя [10. С. 166]. Правда, это немедленно вызвало возражения, поскольку тот же Хайдеггер, к примеру, не считал себя экзистенциалистом вообще, но это не отменяет того факта, что для одних религиозные постулаты (в том или ином виде) были важны, в то время как другие исходили во всех своих построениях из идеи отсутствия бога. Тем не менее вывод, который делают экзистенциалисты из атеизма, доволь-

но неожидан. Жан-Поль Сартр цитирует известную фразу Достоевского о том, что «если бога нет, то все позволено». Однако эта фраза вызывает у него отнюдь не ужас, как у автора цитаты. Сартр воспринимает ее сугубо положительно. Для него такое положение вещей означает одно – у человека нет никаких «оправданий и извинений» [10. С. 169]. Человеку больше не на что сослаться, ему не на кого переложить ответственность. Напротив, за каждый свой поступок он вынужден брать ответственность сам. Парадоксальным образом, от отсутствия бога ответственность человека многократно возрастает, а не исчезает. Отсутствует объективная, внешняя по отношению к человеку мораль – но это вовсе не означает отсутствия норм поведения. Просто эти нормы человек устанавливает для себя сам. «Действительность будет такой, какой ее определит сам человек» [10. С. 172]. Если мы вернемся к описанному нами казусу создания человеком искусственного интеллекта, который необходимо признать живым, мы увидим, что вышеизложенный парадокс Сартра относится к нему в полной мере. Логических следствий из него может быть два. Либо мы пытаемся сформулировать какое-то иное определение жизни (что, как мы уже видели, непросто), и после этого ждем, когда развитие науки и технологии снова поставит перед нами все тот же вопрос, либо мы пересматриваем устоявшиеся представления о взаимоотношениях между богом и человеком. В крайнем проявлении мы признаем человека (ну, может быть, не конкретного человека, а человечество в целом) богом. Если это кажется слишком смелым, мы будем так или иначе вынуждены пересмотреть тезис об эксклюзивности божественной прерогативы творения, а это может вызвать цепную реакцию весьма далеко идущих логических умозаключений. В любом случае мы можем констатировать, что традиционной религии в знакомом нам виде приходит конец, а человек оказывается свободен и обременен ответственностью во вполне сартровском смысле («человек – это свобода» [10]). Очевидно, имеющаяся религия должна либо каким-то образом трансформироваться, чтобы учесть происходящие изменения, либо выбрать путь консервации привычного и стремительной (на памяти считанных поколений) социальной маргинализации. Скорее всего, мы увидим сочетание одного и другого, с одними направлениями, выбирающими путь модернизации (более или менее радикальной), и другими, уходящими в обреченный консерватизм (решив, что «на наш век хватит»). Значение искусственного интеллекта, как мы видим, далеко выходит за рамки его непосредственного физического воздействия – кто, например, знает, куда приведут, какие долгосрочные последствия будут иметь мировоззренческие изменения, о которых мы только что говорили? Причем сами они могут быть с ИИ очевидным образом и не связаны.

4. Искусственный интеллект и экономика. Чуть проще проследить логические причинно-следственные цепочки, которые могут быть запущены применением искусственного интеллекта в тех или иных технологических областях. Их можно назвать последствиями «второго порядка». Сами по себе они могут быть и довольно неожиданными, но на самом-то деле, логика их совершенно прозрачна и целиком вытекает из существующих тенденций развития технологий – и легко прогнозируемого их воздействия на общество.

В самом деле, где может найти себе применение искусственный интеллект? Конечно же, в управлении и контроле за почти любой сферой социальных отношений и деятельности человека. В том числе и производственными отношениями всех видов. Если взять шире, речь может идти вообще о контроле за сложными процессами любого вида.

ИИ как высший продукт цифровых технологий обладает способностью учиться и логическим мышлением, приближенным к человеческому. Он общается с внешним миром и обрабатывает информацию более естественно и гибко, чем прежние программы с заданной рутинной действий. Для этого машине требуется:

- Умение воспринимать и распознавать естественные объекты и речь. В 2017–2018 гг. выведены на рынок распознаватель речи, не уступающий обученным расшифровщикам, и обучает компьютер распознавать объекты в видеозаписи и на фотографии с той же точностью, с какой это делает человек.

- Способность выделять основную информацию и подбирать релевантную. Реклама в стиле «вас также может заинтересовать» строится как раз по такому принципу: программа не только выдает запрошенную информацию, но и делает выводы о том, что еще может оказаться релевантно для клиента. По такому же принципу будет работать «личный секретарь» – ИИ – с той разницей, что подбор информации и предложения будут максимально индивидуализированы.

- База данных состоит не из набора объектов, а из графов, то есть объектов и всей совокупности связей между ними. Именно это позволяет ИИ распознавать паттерны и затем сопоставлять с ними поступающую информацию, то есть ИИ, как и человек, делает выводы на основании своего опыта (базы данных). Принципиальное отличие ИИ, залог его обучаемости – способность исследовать не только объекты, но и совокупность отношений, которые неисчерпаемы.

- Обучение ИИ строится по человеческому принципу нейронной сети – формирования связей между отдельными ячейками памяти. «Очеловечивание» ИИ нужно не для того, чтобы заменить человека или установить контроль высшего разума, а чтобы машина могла наилучшим способом помогать человеку. Одно из основных направлений исследований и усовершенствований – «личный секретарь». В мире будущего такой помощник будет у каждого.

Вслед за Siri от Apple компания Microsoft вывела на рынок Cortana, а Yandex разработал Алису. Эти голосовые ассистенты ищут нужную информацию, распознавая запрос в любой формулировке и учитывая все прежние запросы, оповещают о важных событиях, выполняют рутинную работу. Компании предвидят в дальнейшем развитие самостоятельных ИИ систем, которые будут подбирать и выкладывать «на стол» по запросу своего пользователя: новости и выжимки из документов, общаться друг с другом, составляя график встреч, меню ужина, маршруты отпуска и т. д. То есть ИИ узнает своего пользователя и сможет наилучшим образом подготовить принятие решений.

Особая роль отводится ИИ в сопровождении инвалидов. Уже разработаны программы, восполняющие недостающие зрение, слух или речь, «сами знающие», какая помощь нужна в тот или иной момент. Это направление разработок способствует индивидуализации с учетом конкретных потребностей заказчика. Первый

синтезатор речи, сделанный для Стивена Хокинга в 1985 г., не только совершенствовался в плане управления по мере того, как Стивен утрачивал подвижность сначала пальцев, а потом и мимических мышц, но и подстраивался под пациента, распознавая типичные для него паттерны мысли и выражений. Умение распознавать паттерны и делать на этом основании выводы позволяет внедрять ИИ во все сферы, где требуется осмысленная обработка больших объемов информации. В ближайшие 20 лет искусственный интеллект возьмет на себя рутинную, поисковую и подготовительную работу в логистике, медицине, юриспруденции, образовании, управлении. Он будет предлагать человеку готовые решения с учетом выбиравшихся ранее стратегий. Это возлагает на компании и официальные органы двойную ответственность: просвещать, распространять знания, чтобы люди не чувствовали отчуждения в «дивном новом мире», а напротив, могли воспользоваться его возможностями – и готовить законодательные акты и формулировать этику, сохраняющую при новом мироустройстве основополагающие человеческие ценности.

Бесспорно, сфера образования предоставляет простор для применения технологий искусственного интеллекта, если, конечно, ИИ будет вооружен полным спектром «периферических» технологий, которые позволят ему выполнять свои функции качественно и эффективно. С точки зрения рядового потребителя образовательных услуг это будет означать заметное увеличение их качества, да и доступности тоже (ведь ИИ не устает, не болеет и не уходит в отпуск). Образование на самом деле основной стержень человеческой цивилизации. Именно от степени развития системы образования зависит успешная экономическая составляющая государства и его общества в целом. Именно то, каким образом знания преимущественно получают и в дальнейшем используются людьми во многом определяет то, как они живут. Образование задает рамки нашего существования.

На сегодняшний день применение искусственного интеллекта в образовании в основном сконцентрирована в следующих направлениях:

1. При изучении языков. С Siri можно попрактиковаться в диалоговом режиме, в форме «вопрос-ответ», но если нет словарного запаса работать с программой на английском будет сложно. Совсем другое дело проект Parla, программа использует аккаунт пользователя для выбора необходимого плана обучения.

2. Чат-боты, которые способны осуществлять различные виды деятельности в том числе и образовательные функции. Бота обучают двумя способами: традиционным, то есть вручную более сложным, с подключением искусственного интеллекта: бот в автоматическом режиме самообучается на определенных массивах, типичных ответах и вопросах. Например, Aimylogic – мощный и удобный конструктор для создания чат-ботов с искусственным интеллектом. На сегодняшний день аналогичных платформ, предлагающих чат-боты с ИИ, которые можно обучить и внедрить в образовательный процесс уже очень много.

3. Proctoring или ProctoredTest – механизм, который обеспечивает честность ученика и не дает ему обмануть того, кто принимает экзамен. На помощь пришел искусственный интеллект, который отслеживает одновременно множество сдающих. Платформа Stepik – на данный момент единственная русскоязычная

образовательная онлайн-платформа, где любой желающий может создать экзамен с прокторингом (онлайн-сопровождением и контролем учащегося). При этом такой экзамен может иметь заданную продолжительность, ограниченное время на прохождение, точную дату начала. В перспективе контрольные функции будут осуществляться ИИ через персонализированный видеоанализ внешних параметров экзаменуемых.

4. Еще одно, и наиболее эффективное, направление которое будет развиваться в будущем – игровой обучающий контент на основе ИИ, который сам определит вектор обучения, проанализирует результаты и выстроит необходимый тренд для развития навыков и способностей. Первые шаги в этом направлении осуществляет программная система ИИ Алиса от Yandex, в процессе прохождения игровых квестов, конечно, такой формат перспективно использовать в учебном процессе.

Определяя развитие современного образования необходимо обратить внимание на новые векторы развития искусственного интеллекта в поисковых системах. Современные интеллектуальные поисковые системы в основном используются как помощники пользователя, позволяя быстро находить информацию в сети, показывая наиболее вероятные варианты поискового запроса. Использование данных систем в образовании активно развивается. Например, в изучении иностранных языков. Эволюция данного направления сулит обществу невероятные результаты в будущем цифрового образования. Современные поисковые помощники развиваются за счет самобучения поисковых ИИ-моделей согласно данным запросов пользователей, что, конечно же, ограничивает их потенциал. Необходима смена вектора обучения ИИ, разработка новой парадигмы обучения, при которой будет учитываться информация по цитированию, упоминанию и обсуждению документов, в том числе и к данным из других каналов и приложений пользователя. Можно с уверенностью сказать, что поисковые системы будут определять дальнейшее развитие и Интернета, и цифрового формата образования.

Наиболее близким к новой парадигме развития поисковых систем ИИ будет программируемая low-code ИИ платформа, основными составляющими элементами которой являются:

1. Браузер, в котором система интеграции имеет открытый характер. Это позволит адаптировать новые приложения, а интегрированные приложения получат возможность использовать для своих нужд данные автоматического поиска и соответственно становятся приложениями нового поколения.

2. Система дополненного вебсерфинга, позволяющая осуществлять свою навигацию в Интернете в соответствии со своими интересами, вне зависимости от ссылок, заложенных на сайтах.

3. Встроенный ИИ, анализируя результаты поиска своих пользователей, находит среди них единомышленников, помогает установить между собой контакт.

4. Также платформа, используя персональное облако пользователя, взаимодействует с Интернетом вне зависимости от его онлайн-статуса, информируя о новых событиях и результатах поиска уведомлениями, отправляемыми на устройства пользователя.

Low-code ИИ платформа трансформируется в поисковую систему, позволяющую прогнозировать развитие информационных потребностей у пользователей. Возможности позволяют «доучить» пользователя до определенного им уровня. В платформу интегрируется бот-интерфейс, который самостоятельно определяет необходимые направления в обучении. Пользователь, пролистывая виджеты, только выбирает нужный контент, изучает учебный материал в удобном ему формате, а при включении режима подсказки появляется возможность адаптивного обучения. Используя режим подсказки, пользователь сможет получить необходимые ему данные, а выявленные пробелы будут заполняться предоставляемыми ему дополнительными материалами. Данная система может самостоятельно расширять свои виджеты, используя алгоритм поиска и предоставления информации через обработку результатов освоения учебного контента ИИ системы ассистентом за счет интеграции обучающих программ, при которых пользователь значительно повысит свой уровень.

Искусственный интеллект, таким образом, является очевидным способом решения целого ряда задач стоящих перед современным обществом. Конкретно сферу образования он способен преобразить едва ли не сильнее, чем любую другую, и влияние искусственного интеллекта на нее будет поистине огромным, даже в том случае, если этой сферой Artificial Intelligence и ограничится, а это уже сейчас явно не так, поскольку направление этих изменений во многом совпадает с имеющимися и без того тенденциями развития, и эти тренды в будущем, скорее всего, будут поддерживать и усиливать друг друга.

Список литературы

1. Алексеева И. Ю., Никитина Е. А. Интеллект и технологии: монография. М.: Проспект, 2017. 96 с.
2. Ллойд С., Деннет Д., Рассел С., Вильчек Ф. Искусственный интеллект – надежды и опасения. М.: АСТ, 2020. С. 23–24.
3. Вагин В. Н. Знания и убеждения в интеллектуальном анализе данных. М.: Физматлит, 2019. С. 67–79.
4. Давыдов Н. С. Проблемы прогнозирования: технологическая сингулярность // Искусственный интеллект: философия, методология, инновации: сборник трудов X Всероссийской конференции студентов, аспирантов и молодых ученых, 27–28 апреля 2017 г., МИРЭА. С. 230–234.
5. Голдстауб Т. Как договориться с роботом. М.: Дискурс, 2022. 23 с.
6. Илчева В. И. Роль интеллектуальных информационных систем в новой цифровой экономике // Искусственный интеллект: философия, методология, инновации: сборник трудов X Всероссийской конференции студентов, аспирантов и молодых ученых, 27–28 апреля 2017 г., МИРЭА. С. 92–94.
7. Волосова А. В. Технологии искусственного интеллекта в ULS-системах: учебное пособие для вузов. М.: Лань, 2022. С. 38–39.
8. Александрова Е. В., Польшакова Н. В. Автоматизация производственных процессов. Теория и практика решения задач прикладной математики. М.: Бибком, 2022. С. 54–58.

9. Набатчиков А. М., Бурлак Е. А. Экспериментальные исследования прогнозирования случайного выбора человеком // Искусственный интеллект: философия, методология, инновации: сборник трудов X Всероссийской конференции студентов, аспирантов и молодых ученых, 27–28 апреля 2017 г., МИРЭА. С. 42–47.

10. Рябов П. В., Экзистенциализм. Возраст зрелости. М.: Рипол классик, 2022. С. 165–179.

11. Философские проблемы развития искусственного интеллекта: коллективная монография / под ред. А. В. Волобуева, Н. А. Ореховской. М.: Прометей, 2019. 194 с.

12. Challen, John. ID Buggy shows VW EV platform flexibility // Autonomous Vehicle Technology 15.04.2019. URL: <https://www.autonomousvehicletech.com/.../1675-id-buggy...> (дата обращения: 16.03.2022).

13. Trego, Linda. Eight million vehicles forecast to ship with SAE Level 3, 4 and 5 autonomous technology in 2025 // Autonomous Vehicle Technology. 18.04.2018. URL: <https://www.autonomousvehicletech.com/.../839-eight...> (дата обращения: 16.03.2022).

14. Trego, Linda. Cognitive develops 4D radar for self-driving cars // Autonomous Vehicle Technology. 02.11.2018. URL: <https://www.autonomousvehicletech.com/.../1247-cognitive...> (дата обращения: 16.03.2022).

И. В. Мальцев,

кандидат юридических наук, преподаватель,

Сибирский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ

ГОСУДАРСТВЕННЫЕ СИМВОЛЫ В СОДЕРЖАНИИ ЭЛЕКТРОННОЙ ПОДПИСИ

Аннотация. Статья посвящена выявлению вопросов использования государственных символов, в том числе Государственного герба Российской Федерации, при визуализации электронных подписей. Автором рассматриваются варианты нормативного закрепления элементов, входящих в состав отметок об электронной подписи, а также примеры коллизионных правовых норм, включая положения специализированного национального стандарта в области оформления документов и инструкций по делопроизводству.

Ключевые слова: символ, эмблема, Государственный герб Российской Федерации, электронная подпись, отметка об электронной подписи, визуализация

STATE SYMBOLS IN THE CONTENT OF ELECTRONIC SIGNATURE

Abstract. The article is devoted to the problem of using state symbols, including the Coat of arms of the Russian Federation, when visualizing electronic signatures. The author considers the versions of the legal regulation of elements that are an integral part of the electronic signature marks, as well as examples of conflict rules of law,

including the provisions of the specialized national standard in the field of documentation requirements and instructions for paperwork.

Keywords: Symbol, Emblem, COAT of arms of the Russian Federation, Electronic signature, Electronic signature mark, Visualization

Цифровой мир является уникальной площадкой, на которой могут сталкиваться и сосуществовать традиционные и инновационные правовые объекты. Стремительное развитие новых технологий при этом часто опережает процессы осмысления и системного правового регулирования соответствующих ситуаций. Показательным примером является заявленная в настоящей статье проблематика взаимопересечения государственных символов (тех же гербов – условных «ровесников» изобретения бумажного книгопечатания в Европе) и электронных подписей – продукта современной цифровизации. Актуальность и новизна предлагаемого исследовательского ракурса предопределяются отсутствием специальных научных работ по данной теме.

Одним из отличительных признаков государственных символов является особый порядок официального использования [17. С. 245], обусловленный спецификой их правовой природы [16. С. 144–145; 195–201].

Не случайно, что случаи официального использования государственных символов подробно определяются на законодательном уровне, иногда в нормативных правовых актах, имеющих приоритетную юридическую силу. Так, Государственный герб Российской Федерации, его описание и порядок официального использования установлены Федеральным конституционным законом от 25.12.2000 № 2-ФКЗ «О Государственном гербе Российской Федерации» [1]. На уровне субъектов Российской Федерации их государственные символы и порядок их официального использования также устанавливаются законодательно (примеры конституционных законов: Конституционный закон Республики Алтай от 24.04.2003 № 11-9 «О гербе Республики Алтай» [8], Конституционный Закон Республики Ингушетия от 05.03.2001 № 9-РКЗ «О Государственном гербе Республики Ингушетия» [9], Конституционный закон Республики Тыва от 31.12.1996 № 697 «О государственных символах Республики Тыва» [10]).

Соответственно, круг случаев официального использования государственных символов является ограниченным. На примере Федерального конституционного закона «О Государственном гербе Российской Федерации» мы можем выделить несколько групп обязательных или допустимых случаев размещения герба: на документах общегосударственного образца, на бланках и печатях органов государственной власти, фасадах занимаемых ими зданий, в соответствующих служебных помещениях, на денежных знаках, знаках различия, форменной одежде, государственных наградах. Выход за границы этого круга предполагает применение мер административной ответственности, установленных статьей 17.10 Кодекса Российской Федерации об административных правонарушениях [2] в виде административного штрафа (на граждан в размере от 2 тыс. до 3 тыс. руб.; на должностных лиц – от 5 тыс. до 7 тыс. руб.; на юридических лиц – от 100 тыс. до 150 тыс. руб.).

Административная ответственность за неправомерные действия в отношении государственных символов субъектов Российской Федерации определяется соответствующими региональными законами об административных правонарушениях. Например, согласно статье 2.4 Кодекса Республики Татарстан об административных правонарушениях от 19.12.2006 № 80-ЗРТ [7], незаконные действия по отношению к государственным символам Республики Татарстан, в том числе их использование с нарушением установленных правил, также влекут наложение административного штрафа.

Следует отметить, что большинство нормативных правовых актов, посвященных государственным символам Российской Федерации и ее субъектов, принимались в последнем десятилетии XX в., еще в «аналоговую» эпоху. Даже с учетом самых актуальных редакций они до настоящего времени далеко не в полной мере учитывают реалии эпохи цифровой, включая аспекты использования символов в содержании электронных подписей.

Рассматриваемая нами проблема может быть обнаружена, когда электронная подпись (по сути своей – машиночитаемая информация) визуализируется для непосредственного восприятия человеком. Какие же слова и (или) изображения необходимы для такой визуализации?

В пункте 1 части 3 статьи 12 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» [4] предусматриваются специальные требования к криптографическим средствам, используемым для проверки электронной подписи, которые должны показывать содержание подписанного электронного документа, включая визуализацию электронной подписи, содержащую информацию о том, что документ подписан электронной подписью, а также о номере, владельце и периоде действия сертификата ключа проверки электронной подписи.

Указанные положения о визуализации электронной подписи, введенные в Федеральный закон «Об электронной подписи» в 2019 г. (см. [3]), не содержат указаний о необходимости или возможности использования в данном случае каких-либо государственных символов. Вместе с этим, можно полагать, что восьмилетняя законодательная лакуна к 2019 г. оказалась в той или иной степени заполненной – как несовпадающей практикой правоприменения, так и попытками нормативного правового регулирования.

Так, с 01.07.2018 был введен в действие специализированный ГОСТ Р 7.0.97-2016 (утвержден приказом Росстандарта от 08.12.2016 № 2004-ст) [5], систематизирующий требования к оформлению документов, в том числе с применением информационных технологий. В указанном стандарте мы можем найти специальные положения относительно отметок об электронной подписи (реквизит 23).

ГОСТ Р 7.0.97-2016 устанавливает, что отметка об электронной подписи используется при визуализации электронного документа, подписанного электронной подписью, с соблюдением следующих требований:

а) место размещения отметки об электронной подписи должно соответствовать месту размещения собственноручной подписи в аналогичном документе на бумажном носителе;

б) элементы отметки об электронной подписи должны быть видимыми и читаемыми при отображении документа в натуральном размере;

в) элементы отметки об электронной подписи не должны перекрываться или накладываться друг на друга;

г) элементы отметки об электронной подписи не должны перекрывать элементы текста документа и другие отметки об электронной подписи (при наличии).

Определено, что отметка об электронной подписи в соответствии с законодательством Российской Федерации включает фразу «Документ подписан электронной подписью», номер сертификата ключа электронной подписи, фамилию, имя, отчество владельца сертификата, срок действия сертификата ключа электронной подписи.

Вместе с этим, в дополнение к указанным позициям (воспринятым затем в Федеральном законе «Об электронной подписи»), ГОСТ Р 7.0.97-2016 предусматривает, что отметка об электронной подписи может включать в том числе изображение герба, эмблемы органа власти в соответствии с действующим законодательством.

Возможно, авторы национального стандарта предполагали, что участники электронного документооборота, определяя требования к собственным отметкам об электронной подписи, в первую очередь, соотнесут желание разместить там герб или эмблему с положениями профильных законов, регламентирующих случаи официального использования государственных символов. Однако получившаяся конструкция указанной нормы со ссылкой на действующее законодательство, на наш взгляд, содержит выраженный намек на предварительно проверенную законодательную допустимость размещения гербов или эмблем, что может дезориентировать правоприменителя.

Однако, к сожалению, безотносительно к осмыслению и урегулированию соответствующих случаев использования государственных символов на уровне профильных законов, положения национального стандарта по оформлению документов, определяющих состав отметок об электронной подписи с возможностью изображения гербов и эмблем, стали «прорасти» в ведомственные приказы и региональные подзаконные правовые акты.

При этом, помимо сценариев, когда те или иные инструкции по делопроизводству (1) содержат дублирование формулировок ГОСТ Р 7.0.97-2016 (например, постановление Правительства Нижегородской области от 28.12.2018 № 912 «Об утверждении Инструкции по делопроизводству в органах исполнительной власти Нижегородской области и их структурных подразделениях» [13]) или (2) не предусматривают использование государственных символов в содержании отметок об электронной подписи (например, распоряжение Правительства Кировской области от 24.07.2018 № 207 «Об утверждении Инструкции по делопроизводству в органах исполнительной власти Кировской области» [12]), необходимо особо выделить случаи, когда они (3) устанавливают такое использование в качестве обязательного – несмотря на то, что в профильных законах случаи обращения к государственным символам в целях визуализации электронных подписей не предусмотрено, например:

– «отметка об электронной подписи должна включать в себя изображение герба Алтайского края, фразу “Документ подписан электронной подписью”, но-

мер сертификата ключа электронной подписи, фамилию, имя, отчество владельца сертификата, срок действия сертификата ключа электронной подписи» (пункт 3.13 Инструкции по делопроизводству в Администрации Губернатора и Правительства Алтайского края, утвержденной распоряжением Правительства Алтайского края от 02.02.2018 № 22-р [11]);

– «отметка об электронной подписи в соответствии с законодательством Российской Федерации включает изображение герба Камчатского края, фразу “Документ подписан электронной подписью”, номер сертификата ключа электронной подписи, фамилию, имя, отчество владельца сертификата, срок действия сертификата ключа электронной подписи» (пункт 2.8.20 Типовой инструкции по делопроизводству в исполнительных органах государственной власти Камчатского края, утвержденной распоряжением Правительства Камчатского края от 12.11.2018 № 460-РП [15]);

– «отметка об электронной подписи должностных лиц Правительства Севастополя в соответствии с законодательством Российской Федерации содержит герб Российской Федерации, фразу “Документ подписан электронной подписью”, номер сертификата ключа электронной подписи, фамилию, имя, отчество владельца сертификата, срок действия сертификата ключа электронной подписи» (пункт 20 Инструкции по делопроизводству в Правительстве Севастополя, исполнительных органах государственной власти города Севастополя, утвержденной постановлением Правительства Севастополя от 10.09.2018 № 590-ПП [14]).

Как можно заметить, в последнем примере на региональном уровне затрагиваются вопросы исключительной компетенции Российской Федерации, урегулирование которых допустимо в соответствии с Федеральным конституционным законом «О Государственном гербе Российской Федерации».

Возможно предположить, что на протяжении последних лет снижению «бдительности» по рассматриваемому кругу вопросов способствовало и внедрение форматов визуализации электронных подписей в рамках межведомственного электронного документооборота. В частности, примеры отметок об электронной подписи с «предустановленным» в их содержании Государственным гербом Российской Федерации были установлены совместным приказом Минкомсвязи России № 186, ФСО России № 258 от 27.05.2015 «Об утверждении Требований к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде» (утратил силу в 2021 г.) [6].

Таким образом, поиск наиболее рационального решения проблемы о включении государственных символов в содержание отметок об электронной подписи необходимо продолжать, стремясь к ее системному урегулированию. При этом, на наш взгляд, механическое обращение лишь к формальной стороне вопроса (например, когда его решение будет заключаться во включении в профильные законодательные акты случаев использования символов при визуализации электронных подписей) является недостаточным. Необходимо помнить также, что если мы говорим об оформлении официальных документов (в целом!), то содержание отметки об электронной подписи как одного из реквизитов документа должно быть сопоставлено с другими его реквизитами для исключения элементарного дублирования

информации. Так, в упомянутом выше ГОСТ Р 7.0.97-2016 в качестве реквизита 01 определен герб (Государственный герб Российской Федерации, герб субъекта Российской Федерации, герб (геральдический знак) муниципального образования), а реквизитом 02 является эмблема. Как раз в этих случаях законодательство допускает их размещение на официальных бланках (см., например, статью 3 Федерального конституционного закона «О Государственном гербе Российской Федерации»).

Список литературы

1. О Государственном гербе Российской Федерации: Федеральный конституционный закон от 25.12.2000 № 2-ФКЗ // Собрание законодательства Российской Федерации. – 2000. – № 52. – Ч. I. – Ст. 5021.
2. Кодекс Российской Федерации об административных правонарушениях // Собрание законодательства Российской Федерации. – 2002. – № 1. – Ч. 1. – Ст. 1.
3. О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»: Федеральный закон от 27.12.2019 № 476-ФЗ // Собрание законодательства Российской Федерации. – 2019. – № 52. – Ч. I. – Ст. 7794.
4. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 15. – Ст. 2036.
5. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов. – М.: Стандартинформ. – 2018.
6. Об утверждении Требований к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде: приказ Минкомсвязи России № 186, ФСО России № 258 от 27.05.2015. – URL: <http://publication.pravo.gov.ru/Document/View/0001201509240021> (дата обращения: 08.09.2022).
7. Кодекс Республики Татарстан об административных правонарушениях от 19.12.2006 № 80-ЗРТ // Ватаным Татарстан. – 2006. – 23 дек.
8. О гербе Республики Алтай: Конституционный закон Республики Алтай от 24.04.2003 № 11-9 // Звезда Алтая. – 2003. – 20 мая.
9. О Государственном гербе Республики Ингушетия: Конституционный Закон Республики Ингушетия от 05.03.2001 № 9-РКЗ // Ингушетия. – 2001. – 28 июня.
10. О государственных символах Республики Тыва: Конституционный закон Республики Тыва от 31.12.1996 № 697 // Тувинская правда. – 1997. – 14 янв.
11. Об утверждении Инструкции по делопроизводству в Администрации Губернатора и Правительства Алтайского края: распоряжение Правительства Алтайского края от 02.02.2018 № 22-р. – URL: <http://www.consultant.ru/regbase/cgi/online.cgi?req=doc&cacheid=D30F01359D14E8E21909BD7411950B92&SORTTYP E=0&BASENODE=23568-3&base=RLAW016&n=76277&rnd=V6ZguDT11kXMNb n7#oPhguDTEFrDEqux71> (дата обращения: 08.09.2022).
12. Об утверждении Инструкции по делопроизводству в органах исполнительной власти Кировской области: распоряжение Правительства Кировской об-

ласти от 24.07.2018 № 207. – URL: <https://kirovreg.ru/publ/AkOUP.nsf/62bd0840256f32bcc3257149006da49f/b0b844c02e808191432582da00529dba?OpenDocument> (дата обращения: 08.09.2022).

13. Об утверждении Инструкции по делопроизводству в органах исполнительной власти Нижегородской области и их структурных подразделениях: постановление Правительства Нижегородской области от 28.12.2018 № 912. – URL: <http://publication.pravo.gov.ru/Document/View/5200201812280005> (дата обращения: 08.09.2022).

14. Об утверждении Инструкции по делопроизводству в Правительстве Севастополя, исполнительных органах государственной власти города Севастополя: постановление Правительства Севастополя от 10.09.2018 № 590-ПП. – URL: <http://publication.pravo.gov.ru/Document/View/9200201809180008> (дата обращения: 08.09.2022).

15. Об утверждении Типовой инструкции по делопроизводству в исполнительных органах государственной власти Камчатского края: распоряжение Правительства Камчатского края от 12.11.2018 № 460-РП. – URL: <https://docs.cntd.ru/document/553219956> (дата обращения: 08.09.2022).

16. Мальцев И. В. Символы в праве, правовой науке и юридическом образовании: монография. – М.: Норма, ИНФРА-М, 2022.

17. Юридическая техника: учебник / под ред. В. М. Баранова. – М.: Проспект, 2021.

А. И. Мезенцева,
старший преподаватель,
Черноморское высшее военно-морское ордена
Красной звезды училище имени П. С. Нахимова

ПАТЕНТ КАК СРЕДСТВО ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ ИТ-РАЗРАБОТОК В СФЕРЕ ТЕХНИЧЕСКОГО ОБРАЗОВАНИЯ

Аннотация. В статье описываются патент как средство защиты интеллектуальной собственности ИТ-разработок в сфере технического образования. Аргументируется роль программного обеспечения в современном российском обществе. Описываются права интеллектуальной собственности. Автором приводится классификация объектов интеллектуальной собственности. Определяется место технологий в числе наиболее патентуемых в мире. Приводится личный опыт автора по получению патента на программный продукт.

Ключевые слова: патент, средство, защита, интеллектуальная собственность, ИТ, разработка, техническое образование

PATENT AS A MEANS OF IT DEVELOPMENTS PROTECTING INTELLECTUAL PROPERTY IN THE TECHNICAL EDUCATION FIELD

Abstract. The article describes a patent as a means of intellectual property protection for IT developments in the field of technical education. The article argues the role of software in modern Russian society. Intellectual property rights are described. The author

gives a classification of intellectual property objects. The place of technologies among the most patentable in the world is given. The author's personal experience of obtaining a patent for a software product is given.

Keywords: Patent, Means, Protection, Intellectual property, IT, Development, Technical education

В настоящее время роль программного обеспечения как важного элемента прав интеллектуальной собственности активно обсуждается в России. Текущие дебаты показывают, насколько важен для мирового сообщества вопрос предоставления патентной защиты информационных разработок.

А. Р. Белоусов, первый заместитель Председателя Правительства Российской Федерации, в 2020 г. в своей речи на выступлении на Коллегии Роспатента заявил, что «в сегодняшней ситуации права интеллектуальной собственности стали ведущим экономическим ресурсом наряду с данными, тем экономическим ресурсом, от использования которого в значительной мере зависит решение всех остальных задач, в том числе и задач благосостояния, и задач обороны» [2. С. 143].

Объекты авторского права нуждаются в защите от копирования и несанкционированного использования. С этой целью ИТ-сектор подпадает под действие закона об авторском праве. Кроме того, интеллектуальную собственность защищает патентное право. Патентное право защищает технологию изобретения или программный код.

Объектами интеллектуальной собственности в сфере информационных (ИТ) технологий могут быть объекты права, представленные на рис. 1.



Рис. 1. Объекты интеллектуальной собственности

Авторы интеллектуальной собственности – разработчики продукта. Регистрировать интеллектуальную собственность необходимо для избегания ее копирования или присвоения другими лицами.

На данный момент статистика показывает, что наиболее часто в мире патентуют компьютерные технологии (рис. 2).

<p>Компьютерные технологии (с 2007 по 2017 г. количество патентных документов увеличилось в 1,8 раза, с 125 073 до 229 269 патентных документов в 2007 и 2017 гг. соответственно).</p> <p>Электроника, энергетика (с 2007 по 2017 г. количество патентных документов увеличилось в 1,9 раза, с 102 410 до 197 645 патентных документов в 2007 и 2017 гг. соответственно).</p> <p>Измерительная техника (с 2007 по 2017 г. количество патентных документов увеличилось в 2,2 раза, с 66 697 до 148 809 патентных документов в 2007 и 2017 гг. соответственно).</p>

Рис. 2. Место технологий в числе наиболее патентуемых в мире

Первый в мире патент на IT-разработку был выдан Мартину Готцу (Martin A. Goetz) (США) 23.04.1968: патент № 3,380,029 на SortingSystem5 [6]. В настоящее время каждый год все больше патентов регистрируется в базе России.

Например, автором статьи был разработан программный продукт (ПП) «English Language. Short Course in Physics» по дисциплине «Иностранный язык». Разработанный ПП позволяет эффективно сформировать навыки у обучающихся к коммуникации в устной форме по профессиональной тематике. Активному усвоению иностранного языка с помощью ПП способствуют средства наглядности, которыми полон данный продукт. В процессе освоения ПП обучающиеся запоминают устойчивые выражения, клишированные фразы, специальную терминологию, принципы построения специфических фраз научной терминологии на английском языке [3. С. 9]. Данный ПП отличается авторское оформление контента ПП: информация в нем подается в виде речевых параллелей, что помогает обучающимся запоминать и говорить готовыми фразами на иностранном языке. Программа предназначена для всех участников образовательного процесса. Тип ЭВМ: IBM PC-совмест. ПК; ОС: высокий Windows, Linux, BSD, MacOS [1].

Предложенный программный продукт «Английский язык: краткий курс физики» позволяет изучить и закрепить терминологию научно-технического языка [5. С. 110].

Форма данного ПП также авторская: в конце каждого занятия есть кнопка «Содержание», что позволяет быстро вернуться в начало ПП. В его контент входит таблица Глоссарий /Glossary (рис. 3).

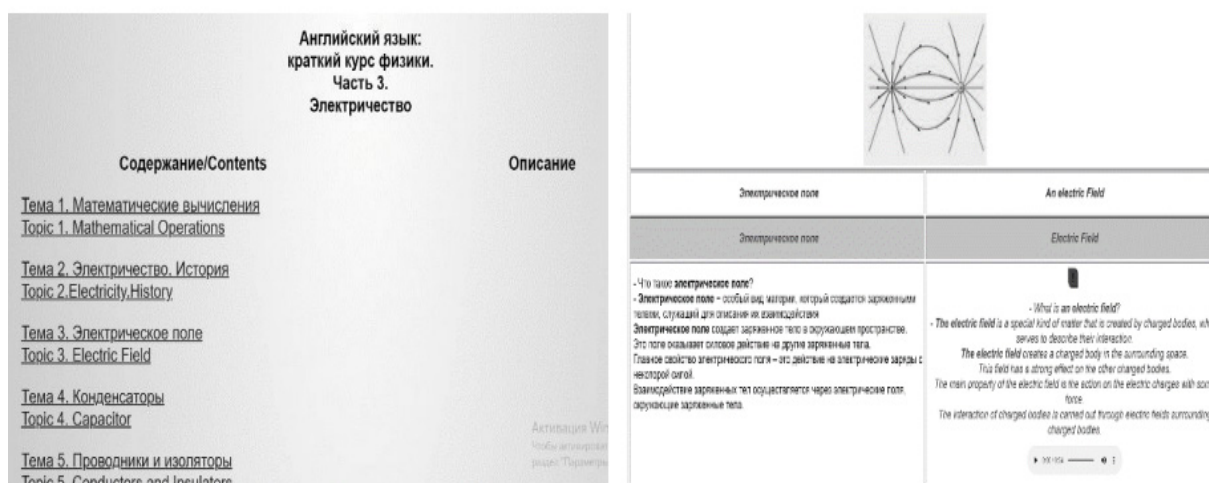


Рис. 3. Программный продукт «Английский язык: краткий курс физики»

В связи с этим на данный программный продукт было решено получить патент [4] (рис. 4).

Итак, необходимо упомянуть, почему стоит получить патент. Получение патента обеспечило защиту интеллектуальной собственности от копирования и присвоения другими лицами. Кроме того, стоит отметить, что обладание патентом дает преподавателю дополнительные баллы и повышает его профессиональный уровень, является преимуществом при повышении квалификации и продолжении образования, а также помогает продвинуться по карьерной лестнице.



Рис. 4. Патент на программный продукт «Английский язык: краткий курс физики»

Список литературы

1. Гордиенко Т. П., Смирнова О. Ю., Мезенцева А. И. Английский язык: краткий курс физики. Электричество. Программный продукт – 2019665747; заявлено 07.11.2019; опубл. 28.11.2019.
2. Ивлиев Г. П. Трансформация сферы интеллектуальной собственности в современных условиях. Москва: Издательский Дом «Городец», 2020. 336 с. <https://rospatent.gov.ru/content/uploadfiles/transformation-ip-2020.pdf>
3. Мезенцева, А. И. Программный продукт как эффективное средство обучения дисциплине «иностраный язык» / А. И. Мезенцева, А. Г. Михайлова, Т. А. Кокодей // Современные социально-экономические процессы: проблемы, тенденции, перспективы: сборник статей X Международной научно-практической конференции, Петрозаводск, 07 марта 2022 г. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И. И.), 2022. С. 7–12. EDN WVHVQJ
4. Свидетельство о государственной регистрации программы для ЭВМ № 2019665747 Российская Федерация. Программный продукт English Language: a Short Course in Physics: № 2019664496: заявл. 07.11.2019: опубл. 28.11.2019 / Т. П. Гордиенко, О. Ю. Смирнова, А. И. Мезенцева. EDN GRZJTT
5. Смирнова О. Ю. Методические основы создания программных продуктов // Проблемы современного педагогического образования. Сер.: Педагогика и психология: сборник научных трудов: Ялта: РИО ГПА, 2017. Вып. 55. Ч. 2. С. 105–113.
6. Goetz, M. A. Applied Data Research Inc, 1968. Sorting system. U. S. Patent 3,380,029.

Л. Е. Мистров,

доктор технических наук, доцент

Центральный филиал Российского государственного
университета правосудия

МЕТОД ЦИФРОВЫХ ТЕХНОЛОГИЙ ДЛЯ МОДЕЛИРОВАНИЯ ЗАДАЧИ СИНТЕЗА СУДЕБНЫХ РЕШЕНИЙ ПО РАЗРЕШЕНИЮ КОНФЛИКТОВ

Аннотация. Предлагается метод применения цифровых технологий (ИТ) для автоматизации судебного процесса по разрешению правовых конфликтов. Основными предпосылками перехода к автоматизации являются: а) логическое представление процесса в виде итерационного последовательного процесса выработки решений; б) формализация понятия «оценочная категория» для определения меры ответственности за правонарушение. Критерием качества принятия решения судьи является выбор объективного и справедливого решения, формализуемого на основе критерия Гурвица. Показано, что для определения предпочтительного решения базируется на принципе максимума полезности, реализованного в форме задачи математического программирования. Применение критерия с последовательным уточнением по стадиям судебного разбирательства обеспечил учет целевых функций представителей

субъектов конфликта на основе методов погрупповой оптимизации и инвариантного погружения. Оптимальное решение судьи основывается на принципе, аналогичном принципу оптимальности Беллмана, позволяющем реализовать метод координации решений судьи до и после принятия решения. Метод обеспечивает моделирование процесса принятия решений судьей для различных условий взаимодействия субъектов конфликта.

Ключевые слова: конфликт, судья, представители конфликтующих сторон, разрешение конфликт, конфликтующая система, судебное решение, критерий, моделирование

DIGITAL TECHNOLOGY METHOD FOR SIMULATION OF THE PROBLEM OF SYNTHESIS OF JUDICIAL DECISIONS ON CONFLICT RESOLUTION

Abstract. A method of using digital technologies (IT) to automate the judicial process to resolve legal conflicts is proposed. The main prerequisites for the transition to automation are: a) a logical representation of the process in the form of an iterative sequential decision-making process; b) formalization of the concept of “assessment category” to determine the measure of responsibility for an offense. The criterion for the quality of the judge’s decision-making is the choice of an objective and fair decision, formalized on the basis of the Hurwitz criterion. It is shown that to determine the preferred solution, it is based on the principle of maximum utility, implemented in the form of a mathematical programming problem. The application of the criterion with successive refinement by the stages of the trial ensured that the objective functions of the representatives of the subjects of the conflict were taken into account based on the methods of group-by-group optimization and invariant immersion. The optimal decision of the judge is based on a principle similar to the Bellman principle of optimality, which makes it possible to implement the method of coordinating the decisions of the judge before and after the decision is made. The method provides simulation of the decision-making process by a judge for various conditions of interaction between the subjects of the conflict.

Keywords: Conflict, Judge, Representatives of the conflicting parties, Conflict resolution, Conflict system, Court decision, Criterion, Modeling

Введение. В настоящее время цифровые технологии (далее – ЦТ) находят широкое применение в различных областях человеческой деятельности, решая задачи повышения производительности труда за счет увеличения объема хранимой и скорости обрабатываемой информации. Это обусловило их широкое применение для решения множества многоплановых задач органами судебной власти. Задачи же автоматизации подготовки и принятия судебных решений по разрешению правовых конфликтов, несмотря на апробированную практику применения [1–3], в целях снижения нагрузки судей и повышения качества их работы являются новыми и до настоящего времени не решаются.

Основными предпосылками применения ЦТ в судебной деятельности при разрешении правовых конфликтов являются: а) логическое представление процесса разрешения правового конфликта в виде итерационного последовательного процес-

са выработки и обоснованного принятия решений (далее – ПР); б) формализация, используемого в правотворчестве понятия «оценочная категория» для определения меры ответственности субъектов конфликта за свершенное правонарушение. Данные обстоятельства, с учетом положительного опыта применения ЦТ в стадиях судебного разбирательства (далее – ССР) [1–3], актуализировало проблему разработки методов и средств цифровизации судопроизводства и обеспечения последовательного перехода к онлайн-правосудию. Это определило целевое содержание статьи, направленной на разработку формализованного метода синтеза решений судей по разрешению правовых конфликтов на основе методов ЦТ для принятия объективного и справедливого решения.

1. Основное исследование.

1.1. Обобщенное логическое представление судебного процесса. В соответствии с административным, гражданским и уголовным процессуальными кодексами (далее – АПК, ГПК, УПК) любой судебный процесс (далее – СП) представляется в обобщенном виде логической последовательностью действий.

1. Открыв судебного заседания судья, предварительно изучив материалы представленного дела, предлагает сторонам разрешить конфликт мировым соглашением, в противном случае суд начинает его рассмотрение.

Для совершения от имени представляемого всех процессуальных действий в суде выделяется представитель (адвокат), который на основе сбора и представления необходимых доказательств дает судье пояснения по существу заявления, представляет при необходимости дополнительные доказательства, а также поднимает вопрос об оказании помощи в истребовании письменных и вещественных доказательств и т. п.

2. На ССР адвокат решает задачу убеждения судей в своей правоте на основе представления имеющейся доказательственной базы.

3. Обоснование доводов в суде первой инстанции осуществляется в стадии судебных прений участвующих в деле лиц и их представителей, после которых завершается рассмотрение конфликта. При этом в процессе выступлений заявитель (его представитель – адвокат) и ответчик (подсудимый – его представитель (прокурор, адвокат)) аргументированно обосновывают причину и условия возникновения конфликта.

4. После судебных прений судья для подготовки решения еще раз изучает все материалы по делу, доказательства сторон, допросы свидетелей и т. д. и принимает решение. Оно, с момента его оглашения, приобретает юридическую силу, вступает в действие и может быть обжаловано в течение установленного законом срока. В этом случае, все стадии СП повторяются.

1.2. Анализ методов моделирования судебного процесса. Судебный процесс представляет сложную динамическую систему исходя из поставленной цели, решаемых задач, числа участников судебного процесса (далее – УСП) и их взаимосвязей во времени, предполагающую для ее исследования применение методов математического моделирования. Характерные особенности данной системы обуславливают определенные ограничения на использование известных методов моделирования. Так, например, применение методов статистического моделирования обусловлено наличием значительных трудозатрат по сбору репрезентативных выборок данных, а динамически

изменяющиеся условия (законодательная база, исходные данные об условиях конфликта и т. п.) могут привести к потере адекватности результатов, полученных с помощью создаваемых моделей. Применение интегрированных аналитических моделей затруднено вследствие невозможности осуществления полной формализации причин, структуры и поведения субъектов в конфликте. Наличие разнородных, трудно формализуемых показателей, критериев и стратегий поведения УСП усложняет также применение моделей исследования операций и оптимального управления.

Повышение качества моделирования такого класса систем и выработки стратегий управления ими возможно за счет разработки сложных моделей, ориентированных на решение только некоторых, частных задач, и новых подходов моделирования, опирающихся на применение существующих моделей. Естественно, что оба эти направления основываются на практической реализации возможностей ЦТ.

Одним из наиболее сложных этапов моделирования СП является этап его формализации: состава, структуры и стратегий поведения субъектов конфликта, основания, этапов и юридической квалификации правонарушения. На нем представления специалистов о решаемой задаче, существующие в виде некоторого описательного, чаще всего ментального, представления о составе, структуре и отношениях между субъектами конфликта, должны быть представлены определенного типа математической моделью. Реализация этапа основывается на наличии знаний о применяемых математических методах моделирования и глубоком понимании закономерностей исследуемой задачи. Решение задачи построения формальной модели СП возможно ускорить при привлечении экспертов для его описания в удобной для восприятия форме с использованием терминологии в данной предметной области. Переход от описательной формы представления информации о СП к его формальному представлению осуществляется на этапе формирования модели, в которой каждому его образу ставится в соответствие определенная конструкция некоторой формальной системы. В этом случае окончанию процесса построения описания СП будут соответствовать определенные математические модели на некотором формализованном языке, допускающем однозначную трактовку понятия «оценочная категория».

1.3. Критерий разрешения правового конфликта. Постановка задачи. В общем случае решение судьи представляет итерационную процедуру обоснования критерия эффективности разрешения конфликта в виде [4]:

$$K = K_1 K_2,$$

где K_1 – критерий принятия судьей законного (обоснованного) решения в соответствии с действующим законодательством; K_2 – критерий принятия судьей субъективного решения на основе его внутренних убеждений о справедливости рассматриваемого конфликта, равный $K_{21} < K_2 < K_{22}$; K_{21} – критерий принятия субъективного решения судьи с учетом оправдательных обстоятельств конфликта, $K_{21} < 1$; K_{22} – критерий принятия субъективного решения судьи с учетом отягощающих обстоятельств конфликта, $K_{22} > 1$.

Представление решения судьи в виде данной зависимости позволяет учесть объективные (законность) и справедливые (субъективность) обстоятельства ПР, которым руководствуется судья при разрешении конфликта.

Наиболее общей формой формализации данных критериев является их представление на основе точечно-множественного отображения φ , ставящего в соответствие каждому элементу множества допустимых вариантов решений судьи V_D подмножество рациональных V^{opt} вариантов: $\varphi: V_D \rightarrow V^{opt}, V^{opt} \in V_D$. При этом отображение φ должно характеризовать целевую функцию судьи при разрешении конфликта, легко определяться, ясно отражать физический смысл СП, быть устойчивым к незначительным изменениям условий и слабоформализуемым факторам конфликта.

В [4] показано, что критерии эффективности ПР судьи по разрешению конфликта в значительной степени зависят от характера учитываемых неопределенных и слабоформализуемых факторов. Это позволяет различать процесс ПР судьей в условиях определенности, риска, неопределенности и нечеткости (в смысле Заде). Процесс ПР применительно к первым трем условиям осуществляется при четко определенном множестве вариантов решений V_D и однозначности отображения целевой функции φ .

А. Процесс ПР в условиях *нечеткости* связан с нечеткими представлениями судьи о разрешаемом конфликте, множестве допустимых вариантов его разрешения V_D и стратегиях поведения субъектов конфликта Y , а также с неоднозначностью отображения φ . В зависимости от условий принятия решения критерий ПР судьей формально представляется на основе принципа максимума полезности математической формой в виде:

$$\text{Max} \langle V_D, R \rangle = \text{Arg} \max_{v \in V_D} U(v). \quad (1)$$

При определенной содержательной трактовке полезности решения судьи принцип максимума полезности обеспечивает сведение задачи ПР к задаче математического программирования.

Б. В общем случае задача ПР судьей в условиях определенности представляется следующим образом: определены множество допустимых вариантов V_D и стратегии поведения субъектов конфликта; из множества допустимых вариантов выбирается вариант (в общем случае их может быть несколько), характеризующийся максимальной полезностью. Формально такая задача является задачей математического программирования и представляется зависимостью:

$$V^{opt} = V^{opt}(Y) = \text{Arg} \max_{v \in V_D} U(v, Y). \quad (2)$$

Из (2) следует, что при ПР в условиях определенности применяется принцип предпочтительности, совпадающий по форме с принципом максимума полезности (1).

В. Процесс ПР судьей в условиях *риска* возникает тогда, когда неопределенные факторы стратегий поведения субъектов конфликта представляют случайные величины с известными законами распределения. При этом под риском понимается степень несоответствия свойств и характеристик решения судьи стратегиям поведения субъектов. Существо задачи в этом случае представляется следующим образом: определены множество допустимых вариантов решений V_D и стратегии поведения субъектов конфликта Y , известны законы распределения случайных факторов $\tilde{Y} \subset Y$ этих условий; из множества V_D выбирается один вариант (или несколько вариантов), минимизирующий риск ПР судьей для данных условий кон-

фликта. В этом случае минимум риска формально эквивалентен в определенном вероятностном смысле максимуму полезности решения. Исходя из этого, в зависимости от той или иной содержательной трактовки вероятностного смысла полезности решения, принцип максимума полезности может принимать различную форму.

Анализ приведенных критериев ПР судьей по разрешению конфликта обеспечивает применение для нахождения законного решения принцип максимума полезности, реализованный в форме задачи математического программирования. Для данного случая постановка задачи ПР судьей по разрешению конфликта заключается в выборе предпочтительных вариантов решений $V^{opt} \in VD$ из множества допустимых V_D для $y, y \in Y$ стратегий поведения субъектов на основе критерия Гурвица в виде зависимости:

$$Arg \max_{v \in V_D} [K_2 \min_{y \in Y} K_1(v, y) + (1 - K_2) \max_{y \in Y} K_1(v, y)], \quad (3)$$

где K_2 – коэффициент «справедливости» ПР судьей, определяющий величину его допустимого риска при ПР (находится в пределах $K_{21} < K_2 < K_{22}$); $K_1(v, y)$ – целевая функция (критерий) ПР судьей.

1.4. Метод формализации судебного процесса. В общем случае судебный процесс по разрешению конфликта является итерационным, направленным на последовательное парирование судьей на ССР информационной неопределенности с целью принятия законного решения, уточненного с позиции его субъективной справедливости. Процесс ПР судьей осуществляется в дискретные моменты времени $t = \overline{1, T}$, шаг дискретизации которых в процессе принятия решения варьируется от стадии к стадии. Часть решений, в основном на начальных ССР, направлена на уточнение исходной информации о конфликтующей системе «истец – ответчик» («прокурор – подсудимый»), а другая часть – по координации работы ПС. При этом судьей возможна координация целевых функций ПС (в задаче предполагается, что они определены). При ПР основной целью судьи является нахождение на i -ой, $i = \overline{1, N}$ ССР вектора решений $x_i^o(t)$, который обеспечивает максимум вектора его целевой функции $K_1(v, y, x_1^o, \dots, x_i^o, \dots, x_N^o)$ при координирующей цели $x_{N+1}^o(t)$, определенной судьей. Найденное решение судьи $\{x_i^o\}$, $i = \overline{1, N}$ должно принадлежать подмножеству допустимых решений – соответствовать ст. 6 УПК, ст. 6 ГПК и ст. 297 АПК РФ и должно быть законным и справедливым.

Применение единого критерия $K_1(v, y, \bar{x}_N)$ с последующим уточнением его по ССР усложняет задачу судьи, но позволяет учесть целевые функции ПС (адвокатов, прокурора). К тому же целевая функция судьи $K_1(v, y, \bar{x}_N)$ не зависит в явном виде от решений, формулируемых ПС, что затрудняет их работу при анализе и установлении стратегий поведения субъектов конфликта. Поэтому предполагается, что у каждого j -го ПС на i -й ССР определены цели $K_1(v, y, \bar{x}_{ij})$ на множествах их допустимых решений, а интегральная целевая функция $K_1(v, y, \bar{x}_1, \dots, \bar{x}_N)$ является векторной и зависит как от критерия судьи эффективности $K_1(v, y, \bar{x}_N)$, так и от целевых функций ПС $K_1(v, y, \bar{x}_{ij})$.

Если представить \bar{x}_N в виде $\bar{x}_N = \{\bar{x}_j\}$, $i = \overline{1, N}$, $j = \overline{1, M}$, где $M = m_i$ – число УСП на i -й стадии (в частном случае полагается, что $M = 3$; $j = 1$ – судья, $j = 2$ и 3 – ПС), то предполагается, что при нахождении решений $x_{(i-1)j}$, $j = \overline{1, m_{i-1}}$ все решения \bar{x}_{ij}^o , $j = \overline{1, m_i}$ уже приняты. Поэтому для оптимизации решений судьи возможно использование метода погрупповой оптимизации [например, 5] и метода инвариантного погружения [6]. Это позволяет рассматривать вместо задачи с конкретным решением (планом) x_{N+1}^o на $(N+1)$ -й ССР и фиксированным числом стадий N некоторое семейство задач с $N = 1, 2, 3, \dots$; $x_{N+1}^o = [0, \infty]$. В этом случае максимум функции $K_1(v, y, \bar{x}_1, \dots, \bar{x}_N)$ зависит от значений N и \bar{x}_i , и эту зависимость необходимо установить. Исходя из этого, задача (3) за счет использования метода инвариантного погружения декомпозируется на совокупность задач, связанных с решениями судьи по ССР. При этом в качестве характеристики ПР j -и УСП используется функция принадлежности вариантов принимаемых ими решений подмножеству допустимых ($C \subset X$), эффективных (соответствующих мере наказания за содеянное правонарушение) и скоординированных (удовлетворяющих прокурора (истца) и подсудимого (ответчика)) решений $\mu_R(\bar{x}_N)$. Эта функция не сводится к определению только количественных (четких) значений функции $K_1(v, y, \bar{x}_N)$, так как включает в себя не только характеристику эффективности решения, но и характеристику его допустимости (степень принадлежности решения \bar{x}_N к подмножеству допустимых решений C) и скоординированности с целями и ограничениями ПС (степень принадлежности решения \bar{x}_N к подмножеству скоординированных решений ПС K) на основе методов векторной оптимизации. Функции принадлежности определяются на множестве решений $X = \{x_{ij}\}$. Эффективность решений задается нечеткой целью $G \subset X$ как нечеткое подмножество с функцией принадлежности $\mu_G(x_{ij})$, допустимость решений – нечетким подмножеством $C \subset X$ с функцией принадлежности $\mu_D(x_{ij})$ и скоординированность – нечетким множеством $K \subset X$ с функцией принадлежности $\mu_K(\bar{x}_j)$. Результирующее влияние нечетких цели G , ограничения C и координации K на выбор решения x_{ij} может быть представлено в виде пересечения $G \cap C \cap K$. Тогда функция принадлежности решения судьи к множеству допустимых решений для пересечения задается в виде [7, 8]:

$$\mu_{G \cap C \cap K}(x_{ij}) = \mu_G(x_{ij}) \wedge \mu_R(x_{ij}) \wedge \mu_K(x_{ij}) = \min\{\mu_G(x_{ij}), \mu_R(x_{ij}), \mu_K(x_{ij})\} \quad x_{ij} \in X. \quad (4)$$

Исходя из этого, подмножество $R = G \cap C \cap K$ представимо векторным (нечетким) решением j -х ПС на i -й стадии, причем

$$\mu_R(x_j) = \mu_{G \cap C \cap K}(x_{ij}) \quad (5)$$

При разрешении материального спора между субъектами конфликта решение судьи r -го уровня принятия решения ($j = 1$) на $(i+1)$ -й стадии судебного разбира-

тельства может быть связано с решением ПС на i -й стадии уравнением $x_{(i+1)r} = K_1(v, y, x_{i1}, \dots, x_{iM})$. В случае когда множество решений X состоит только из одного параметра, уравнение представимо в виде:

$$x_{(i+1)r} = \sum_{j=1}^M x_{ij}. \quad (6)$$

Однако решения являются сложными и характеризуются вектором параметров \bar{x}_{ij} , например, имущественным спором P_{ij} , расходом средств q_{ij} и т. п.

Скоординированное с ПС решение судьи на N -й стадии в соответствии с [7] представляется зависимостью:

$$R(x_N) = R(x_{11}) \cdot \dots \cdot R(x_{1M}) \cdot R(x_{21}) \cdot \dots \cdot R(x_{2M}) \cdot R(x_{(N-1)1}) \cdot \dots \cdot R(x_{(N-1)M}) \bigcap C(x_N) \bigcap G(x_N), \quad (7)$$

из которой несложно получить рекуррентную процедуру для ПР судьей на N -й ССР. Вследствие инвариантности введенного описания по ССР из (7) следует, что:

$$R(x_{ij}) = R(x_{11}) \cdot \dots \cdot R(x_{1M}) \cdot R(x_{21}) \cdot \dots \cdot R(x_{2M}) \cdot R(x_{(i-1)1}) \cdot \dots \cdot R(x_{(i-1)M}) \bigcap C(x_{ij}) \bigcap G(x_{ij}), \quad (8)$$

в частности,

$$R(x_{(i+1)r}) = R(x_{11}) \cdot \dots \cdot R(x_{1M}) \cdot R(x_{21}) \cdot \dots \cdot R(x_{2M}) \cdot R(x_{i1}) \cdot \dots \cdot R(x_{iM}) \bigcap C(x_{(i+1)r}) \bigcap G(x_{(i+1)r}). \quad (9)$$

В связи с тем, что решение на i -й ССР зависит только от установленных данных о характеристиках внешних условий и стратегий поведения субъектов конфликта; решений, принимаемых судьей на $(i-1)$ -й стадии и решений ПС, то в решении $R(x_{ij})$ учитываются все стратегии поведения ПС в соответствии с (8). Тогда (9) можно представить через нечеткие решения предыдущей стадии в виде:

$$R(x_{(i+1)r}) = [R(x_{11}) \cdot \dots \cdot R(x_{1M})] \bigcap C(x_{(i+1)r}) \bigcap G(x_{(i+1)r}). \quad (10)$$

Причем для ПР судьей на $(i+1)$ -й стадии он должен предварительно свернуть решения ПС $R(x_{i1}), \dots, R(x_{iM})$ в свое решение $R(x_{i1}, \dots, x_{iM})$. Тогда (10) можно представить в виде:

$$R(x_{(i+1)r}) = R(x_1, \dots, x_{1M}) \bigcap C(x_{(i+1)r}) \bigcap G(x_{(i+1)r}). \quad (11)$$

Наличие такой рекуррентной процедуры обусловлено особенностью ПР судьей и наличием особых законодательно закрепленных прав по получению недостающей информации и ПР. Однако в отличие от общепринятого представления решений в четкой форме – в виде конкретных числовых значений параметров решений, решения ПС в процессе координации их решений являются нечеткими и задаются функциями принадлежности $\mu(x)$. Тогда для функций принадлежности рассматриваемого подмножества эффективных и допустимых решений (11) приобретает вид:

$$\mu_R(x_{(i+1)r}) = \mu_R(x_{i1}, \dots, x_{iM}) \otimes \mu_G(x_{(i+1)r}) \otimes \mu_C(x_{(i+1)r}), \quad (12)$$

где $\mu_R(x_{i1}, \dots, x_{iM}) = \mu_R(x_{i1}) \otimes \dots \otimes \mu_R(x_{iM})$. (13)

Бинарная операция \otimes может быть представлена конкретной алгебраической операцией. Выбор операции обуславливается типом операции над множествами, физическим смыслом функций принадлежности и аксиоматикой нечетких множеств.

Функция принадлежности $\mu_R(x_{i1}, \dots, x_{iM})$ характеризует согласно (4) координацию K судьей решений ПС, причем для ПР на $(i+1)$ -й стадии необходимо спроектировать координирующее решение судьи $\mu_R(x_{i1}, \dots, x_{iM})$ на ось $x_{(i+1)r}$ с учетом (6). Тогда функцию $\mu_R(x_{i1}, \dots, x_{iM})$ можно представить в виде:

$$\mu_K(x_{(i+1)r}) = \mu_R\left(\sum_{j=1}^M x_{ij}\right). \quad (14)$$

Уравнение (14) показывает, что решение судьи $x_{(i+1)r}$ основывается на учете решений ПС x_{i1}, \dots, x_{iM} и оно будет эффективным, когда каждый представитель на i -й стадии принимает оптимальные решения (максимизирует свою функцию принадлежности), а судья при определении своего решения стремится максимизировать проекции этих решений на ось $x_{(i+1)r}$, т. е.:

$$\mu_K\left(\sum_{j=1}^M x_{ij}\right) = \max_{\{x_{ij}\}} [\mu_R(x_{i1}) \otimes \dots \otimes \mu_R(x_{iM})]. \quad (15)$$

При этом оптимальное решение судьи обладает тем свойством, что каковы бы ни были состояние и решение на предыдущей ССР в момент t , последующие решения должны быть оптимальными относительно этого решения. Это дает возможность характеризовать оптимальную стратегию судьи при поиске оптимального решения на основе принципа, аналогичного принципу оптимальности Беллмана [9]. Применение данного принципа оптимальности позволяет реализовать эффективный метод координации решений, принимаемых на отдельных ССР, сократить до минимума обмен информацией между стадиями и обеспечить автономную работу с информацией ПС.

На основе этого принципа определим рекуррентную процедуру ПР судьей на $(i+1)$ -й стадии, которая включает три этапа.

1. Решается оптимизационная задача на декартовом произведении множеств $x_{i1} \times \dots \times x_{iM}$ с целевой функцией (15) на $(i+1)$ -й стадии с учетом ограничения (6). Так как ПС на i -й стадии связаны между собой материальными потоками, то ограничение (6) дополняется системой ограничений – равенств и ограничений – неравенств вида:

$$\overline{M}(x_{i1}, \dots, x_{iM}) = 0; \quad \overline{W}(x_{i1}, \dots, x_{iM}) \geq 0, \quad (16)$$

описывающих связь стратегий поведения ПС на i -й стадии.

Результатом решения задачи является функция принадлежности

$$\mu_K(x_{(i+1)r}) = \mu_R\left(\sum_{j=1}^M x_j\right). \quad (17)$$

2. Находится нечеткое решение судьи на $(i+1)$ -й стадии $\mu_K(x_{(i+1)r})$ на основе (12) и (13). Для принятия четкого решения судьей на N -й стадии необходимо выбрать такое решение x_N^o , для которого степень принадлежности к подмножеству эффективных и допустимых решений $\mu_R(x_N)$ является максимальной, т. е. $\mu_R(x_N) = \max_{\{x_N\}} \mu_R(x_N)$.

После принятия четкого решения на N -й стадии на основе решения оптимизационной задачи (15) и (16) при $\sum_{j=1}^M x_{(N-1)j} = x_N^o$ находятся четкие решения на $(N-1)$ -й стадии $x_{(N-1)j}^o, \dots, x_{(N-1)M}^o$. Далее эта процедура повторяется до тех пор, пока не будут четко и количественно приняты все решения судьей $\{x_{ij}\}$, $i = \overline{1, N}$, $j = \overline{1, M}$.

3. При невыполнении условия (16) ПС может быть опротестовано решение судьи и задача подлежит рассмотрению апелляционным или кассационным судом с учетом полученной информации и решения суда первой инстанции.

Решения ПС могут являться элементарными и не иметь координирующих функций, то есть $\mu_K(x_{1r}) = 1$, $r = \overline{1, M}$. Их активность проявляется в получении недостающей информации и формирования на ее основе своих нечетких решений $R(x_{1r}) = C(x_{1r}) \cap G(x_{1r})$.

Вследствие наличия взаимосвязи ПС через СП возникает необходимость координации их решений, исходя из целевой функции и моделей, описывающих этот процесс. В этом случае координирующая функция может быть получена на основе решения оптимизационных задач для сложных информационных процессов.

Целевые функции судьи на каждой ССР являются специфическими и состоят в обеспечении эффективной работы ПС $\mu_G(x_{(i+1)r}) = 1$.

Так как судья имеет единую цель G , то при ПР она учитывает цели и возможности ПС через координирующее нечеткое решение $\mu_K(x_{(i+1)r})$ в формуле (4). Эта функция принадлежности обеспечивает гарантированные условия работы ПС, т. е. фактически отражает факт учета их интересов в процессе ПР.

В общем случае функция принадлежности $\mu(x_{ij})$ может быть условной, то есть зависеть от некоторого параметра $y_{ij} - \mu(x_{ij} / y_{ij})$. Например, если x_{ij} есть учет временных параметров конфликта на i -й стадии, то y_{ij} – объем получаемой информации о параметрах разрешаемого конфликта.

Представленная в формализованном виде на основе теории нечетких множеств позиция судьи по парированию информационной неопределенности и разрешению конфликта является полностью определенной, так как задана структура конфликта, определены критерии и выделены ССР, выявлены предпочтения для каждого ПС

и судьи в целом путем задания соответствующих функций принадлежности, система уравнений и ограничений, описывающих их связи.

Введение рекуррентной процедуры и наличие в ней трех этапов связано с необходимостью разрешения судьей конфликтов двух видов: внутриуровневого, возникающего из-за несовместимости частных целей отдельных субъектов конфликта в рамках заданной (установленной) его структуры и ограничений, и межуровневого (между судьей и ПС), имеющего место из-за того, что цель судьи не совпадает с целевыми функциями ПС. Эти конфликты разрешаются последовательно с использованием первого и второго этапов рекуррентной процедуры.

Метод позволяет реализовать процесс координации решений судьей, производимый до принятия решения ПС или после ПР (его коррекция после подачи апелляционного или кассационного заявления). С его помощью возможно согласование решений в СП по разрешению споров сторон в конфликте. Судья и ПС связаны между собой двумя видами информации. Информация, получаемая от ПС, несет судье информацию о допустимости и эффективности разрабатываемых решений (нечеткое оптимальное решение), а информация, идущая от него, конкретизирует задачи, выполняемые ПС. Судья в связи с приоритетом действий позволяет уточнить ПС стратегии их поведения (выбор способа координации), внести (доказать) соответствующие изменения в действия и параметры конфликта (аспект самоорганизации) и координирующее воздействие при фиксированных действиях и параметрах (аспект управления). Информация о стратегиях ПС, необходимая судье для ПР, зависит от цели рассматриваемой задачи, стратегий поведения ПС (истца и ответчика) и взаимосвязей между ними. Поэтому для нормальной работы судьи целесообразным является определение стратегий ПС как взаимодействие взаимосвязанных конфликтующих сторон, каждая из которых преследует частные цели. Поэтому при оптимизации ПР судьей должны исследоваться внутриуровневые и межуровневые взаимодействия УСП.

Функции принадлежности УСП удовлетворяют основным требованиям, предъявленным к числовым характеристикам:

- они представляют величины, зависящие от состояния субъектов конфликта и связей между ними, и вычисляются исходя из имеющейся информации о них (детерминированной, вероятностной, лингвистической);

- каждая из функций принадлежности, построенная для субъектов конфликта, дает наглядное представление об одном из их свойств;

- функция принадлежности допускает простую приближенную оценку на основе априорных данных или экспертных оценок.

Использование метода обеспечивает выполнение гомоморфности моделей ПР судьей и ПС. На уровне судьи осуществляется оптимизация задач получения информации по ССР с учетом взаимодействия с ПС и решается оптимизационная задача об эффективности и допустимости рассматриваемых вариантов решений. При анализе конфликта детально рассматриваются только та информация и стратегии ПС, которые приводят к изменению эффективности и допустимости вариантов решений, а все, что не играет особой роли с точки зрения судьи, исключается из дальнейшего рассмотрения. Таким образом, при переходе с одной стадии на другую теряется некоторая информация о параметрах, но появляется возможность судить

о сравнительной важности установленных параметров разрешаемого конфликта. Рассмотрение задач на какой-либо ССР позволяет найти информацию и дать ответ лишь на определенную группу вопросов; каждая из стадий имеет свои, только присущие ей ограниченные информационные возможности.

1.5. Обоснованность принимаемых решений. При разрешении конфликта возникает задача координации решений судьи при реализации поставленной цели с ПС. Конфликт между ПС возникает из-за наличия у них частных целей и из-за различных видов системных ограничений и связей. Действия судьи направлены на снижение внутрисистемного конфликта. Эффективность действий судьи по координации оценивается с помощью введенной функции принадлежности его работы к подмножеству эффективных и допустимых решений. Основная трудность решения задачи состоит в зависимости решений ПС от формулировки со стороны судьи цели, задач и ограничений, а решений судьи, в свою очередь, – от стратегий ПС. Это нестрогое противоречие разрешается введением на уровне ПС оптимального нечеткого решения.

Для количественного расчета эффективности координации решений судьи введем в рассмотрение по аналогии с [8] на языке теории нечетких множеств два понятия координируемости решений.

Как уже отмечалось выше, координируемость решений с использованием функций принадлежности заключается в нахождении таких условий работы судьи x^o , для которых функция принадлежности $\mu_R(x)$ принимает максимальное значение. Следовательно, задача имеет решение, если имеются такие условия x^o , для которых $\mu_R(x^o) \neq 0$, т. е. $\exists x \mu_R \neq 0$.

Решения ПС на i -й стадии описываются функциями принадлежности $\mu_R(x_j)$, $i = \overline{1, N}$, $j = \overline{1, M}$, а решение судьи по координированию решений – функцией принадлежности $\mu_K(x_{(i+1)r})$. Исходя из этого задачи, решаемые ПС в процессе, координируемы между собой в момент времени t тогда и только тогда, когда справедливо: $\forall j \exists x_{ij} \exists x_{(i+1)r} [\mu_R(x_{ij}) \neq 0 \wedge \mu_K(x_{(i+1)r}) \neq 0]$ Следовательно, координируемость задач ПС требует, чтобы рассматриваемая задача имела решение хотя бы при одном $x_{(i+1)r}$ и для этого решения множества частных задач R , решаемых ПС, также имело решение.

Так как функция $\mu_G(x_{(i+1)r})$ является максиминным критерием и выражение (3) можно записать в виде $\exists x_{(i+1)r} [\mu_K(x_{(i+1)r}) \neq 0]$, т. е. в терминах теории нечетких множеств задачи, решаемые ПС, координируемы между собой в том случае, если нечеткое множество R не пусто $\mu_K(x_{(i+1)r}) \neq 0$.

Задачи, решаемые ПС, координируемы относительно формулируемой судьей цели G в судебном процессе в момент времени t , если справедливо предположение:

$$\forall j \exists x_{ij} \exists x_{(i+1)r} [\mu_R(x_{ij}) \neq 0 \wedge \mu_K(x_{(i+1)r}) \neq 0]. \quad (18)$$

Так как $\mu_R(x_{(i+1)r})$ является максиминным критерием, (18) можно переписать в виде $\exists x_{(i+1)r} [\mu_R(x_{(i+1)r}) \neq 0]$.

На основе данных понятий координируемости устанавливается согласованность решений: а) для эффективной работы судьи необходимо, чтобы его цели и задачи ПС были скоординированы между собой и с целью СП; б) судья обладает свойством безусловной межуровневой согласованности, если его управляющие воздействия, максимизирующие согласно принципа оптимальности системную функцию принадлежности, одновременно максимизируют и частные функции принадлежности ПС – это присуще идеально работающему судье. Для реального судьи степень согласованности отличается от 1, и потери при координации работы ПС возможно оценивать разностью между $\mu_R(x_{ij}^o_{\text{сист}})$ и $\mu_R(x_{ij}^o_{\text{авт}})$ под управлением судьи в СП.

Выводы. Применение предложенного метода цифровизации моделирования СП по разрешению конфликта обеспечивает: целостность функционирования судьи при разрешении конфликтов для исследования всей конфликтующей системы (прокурор, истец, подсудимый, ответчик и адвокаты) с позиции единой цели; всесторонность рассмотрения и учета основных элементов и процессов конфликтующей системы и связей между ними; достаточную степень упрощения при моделировании, которая позволяет адекватно отразить СП и учесть определяющие факторы в нем – это связано с тем, что при разработке решений исследуется не сам СП, а его модель. На его основе возможно построение численных процедур проведения расчетов, составляющие методическую основу информационной системы поддержки принятия решений судьей по законному и справедливому разрешению конфликтов.

Список литературы

1. Coronavirus and the courts: how will a pandemic affect the conduct of litigation? // The Lawyer. URL: <https://www.thelawyer.com/coronavirus-and-the-courts-a-boost-for-online-reform>
2. China steps up online litigation services amid coronavirus epidemic // The Star. URL: <https://www.thestar.com.my/news/regional/2020/03/30/china-steps-up-online-litigation-services-amid-coronavirus-epidemic>
3. Китайских судей заменят компьютерные программы. URL: <http://itnews.com.ua/news/25714-kitajskikh-sudej-zamenyat-kompyuternye-programmy>
4. Мистров Л. Е. Метод синтеза судебных решений по разрешению социально-экономических конфликтов // Нелинейный мир. 2014. Т. 12, № 8. С. 54–66.
5. Методы принятия управленческих решений: учебное пособие / под ред. П. В. Иванова. Москва: Юрайт, 2019. 276 с.
6. Лихолетов В. В., Гельруд Я. Д. Управление предприятием (организацией). Методы решения задач и принятия управленческих решений: учебное пособие. Челябинск: ЮУрГУ, 2020.
7. Mistrov L. E., Mishin A. V. Method of Synthesis of the Information Model of the Judicial Decision Support System // R. Silhavy, P. Silhavy, Z. Prokopova (eds). Software

Engineering Perspectives in Intelligent Systems. CoMeSySo 2020. Advances in Intelligent Systems and Computing. Vol. 1295. Springer, Cham, 2020. Pp. 522–530.

8. Алтунин А. Е., Семухин М. В. Модели и алгоритмы принятия решений в нечетких условиях: монография. Тюмень: Изд-во Тюменского государственного университета, 2000. 352 с.

9. Карпов Д. А., Струченков В. И. Динамическое программирование в прикладных задачах, допускающих сокращение перебора вариантов // Russian Technological Journal. 2020. № 8 (4). С. 96–111. УДК 343.7

А. Х. Мямиев,

преподаватель, кафедра цифровой экономики,

Туркменский государственный институт экономики и управления

К. Пердяев,

магистрант, кафедра экономической теории,

Туркменский государственный институт экономики и управления

КОММЕРЧЕСКИЕ УГРОЗЫ В ТОРГОВОЙ СИСТЕМЕ

Аннотация. В данной работе рассмотрен вопрос развития систем повышения безопасности от коммерческих угроз в торговых системах, их особенности и направления развития мер безопасности в торговле. Проведен системный анализ развития цифровых технологий в торговых системах, а также развитие мер по повышению безопасности в торговых сетях. Даны рекомендации по внедрению технологий в отрасль.

Ключевые слова: цифровая экономика, торговля, безопасность, технологии

COMMERCIAL THREATS IN THE TRADING SYSTEM

Abstract. In this paper, the issue of developing security systems from commercial threats in trading systems, their features and directions for the development of security measures in trade was considered. A systematic and analytical analysis of the development of digital technologies in trading systems was carried out, as well as the development of measures to improve security in trading networks. Recommendations are given for the introduction of technologies in the industry.

Keywords: Digital economy, Trade, Security, technology

Предвидение коммерческих рисков в торговой системе – одно из важнейших требований к предпринимателю. Риск – это степень неопределенности исхода. Деловые риски – возможные потери в бизнесе. Определяется как неправильное решение, принятое до отгрузки товара и приводящее к убыткам. Предпринимательские риски включают девальвацию (снижение покупательной способности денег), ухудшение финансового состояния компании, а также заключение опасных контрактов, неисполнение контрактных обязательств конкурентами, уничтожение или повреждение товаров при транспортировке, стихийные бедствия и так далее и могут возникнуть на почве возможной недобросовестности. Кроме того, ком-

мерческие угрозы могут возникать из-за нестабильности общественно-политической ситуации. Невозможно вести бизнес без риска, но планирование должно учитывать последствия коммерческого риска.

В целях минимизации риска следует использовать максимальное количество доступной информации, всесторонне анализировать эффективность коммуникации с партнерами, финансовые результаты и бизнес-операции, всесторонне изучать рынок и тщательно подбирать сотрудников. Разделение приоритетов в коммерции не менее важно, чем в производстве. Реализация этого принципа требует, чтобы все аспекты бизнес-процесса были освоены и известны в любое время. Личное предложение зависит от каждого человека, работающего в коммерческой среде, и определяется не только личными характеристиками, но и учетом их рабочей культуры. Личный характер трейдера составляет основу компетентного характера. Культура работы предполагает определенный уровень организационных основ, она должна быть открыта для инноваций, говорить «нет» старому и быть способной быстро внедрять новые и более эффективные способы общения и ведения бизнеса с сотрудниками и коллегами. Он должен участвовать в рабочей среде, искать новые научно-технические достижения, с энтузиазмом относиться к собственности, уметь быстро осваивать новые методы, которые повысят эффективность работы [1. С. 59].

Высокая ответственность за свои обязательства по коммерческим соглашениям – это принцип, который создает репутацию в деловом мире. Выполнение этого принципа является залогом эффективной торговли. При осуществлении бизнеса его субъекты должны полностью соблюдать действующее законодательство, повышать культуру и качество обслуживания потребителей [2. С. 62].

Коммерческие организации весьма разнообразны по своим функциям, организационно-правовой структуре, степени привлечения иностранных партнеров, масштабам и основным направлениям деятельности. Но, несмотря на это разнообразие, их можно разделить на группы, которые организованы в соответствии с выбранными классификационными критериями [3. С. 80].

Группировка позволяет решить ряд вопросов, в том числе:

- определяет роль каждого предприятия в коммерческом секторе и их цели;
- организует предприятия по сходным признакам;
- правильно оценивает и сравнивает эффективность деятельности предприятия [4. С. 52].

В целях регулирования деятельности хозяйствующих субъектов субъекты торговли могут быть разделены на группы по принятым государством гражданско-правовым нормам, т. е. по правовому положению предприятия, его количественным размерам, виду осуществляемой торгово-хозяйственной деятельности и его личностные особенности. Размер каждой торговой компании влияет на ее производительность. Важно знать экономические преимущества и недостатки каждой из структур различного размера. Исходя из сферы деятельности, необходимо учитывать взаимосвязь между развитием бизнеса и выбором правильной маркетинговой стратегии [5. С. 91].

Список литературы

1. Аброскин, А. С. Международный опыт измерений цифровой экономики / А. С. Аброскин // Вестник университета. 2018. № 12. С. 59–6. URL: <https://elibrary.ru/item.asp?id=36963747>
2. Ахметова, С. Г. Опыт внедрения новых технологий в высшем профессиональном образовании / С. Г. Ахметова, Л. В. Невская // Вестник Пермского национального исследовательского политехнического университета. Социально экономические науки. 2018. № 2. С. 62–69. URL: <https://elibrary.ru/item.asp?id=35193981>
3. Багаутдинова, Н. Г. Новые конкурентные преимущества в условиях цифровизации / Н. Г. Багаутдинова, Р. А. Никулин // Инновации. 2018. № 8. С. 80–83.
4. Барабаш, К. С. Влияние цифровой экономики на изменение рынка труда / К. С. Барабаш // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2018. № 6 (97). С. 52–54.
5. Баранов, Д. Н. Социально-экономические последствия распространения цифровых технологий на рынке труда / Д. Н. Баранов // Вестник Московского университета им. С. Ю. Витте. Серия 1: Экономика и управление. 2018. № 3 (26). С. 91–97.

Л. С. Нижник,

кандидат юридических наук,

доцент кафедры земельного права,

Государственный университет по землеустройству

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПУБЛИЧНО-ПРАВОВЫХ ОТНОШЕНИЙ В СФЕРЕ ЭКОЛОГИИ

Аннотация. В статье исследуется тенденция к законодательному регулированию использования цифровых технологий в публично-правовых отношениях в сфере экологии. Определяя сущность цифровой трансформации названной сферы, выявляются характерные историко-нормативные этапы, значение которых могло сформировать направление по совершенствованию правового регулирования экологических отношений. Сделан вывод, что переход к устойчивой цифровизации призван оптимизировать и усовершенствовать механизм государственного управления в сфере экологии, в том числе выявить результативность и комплексность ее правореализации.

Ключевые слова: цифровая трансформация, экология, экологические правоотношения, цифровизация, публично-правовые отношения, конституционно-правовое обустройство, охрана окружающей среды

DIGITAL TRANSFORMATION OF PUBLIC LEGAL RELATIONS IN THE FIELD OF ECOLOGY

Abstract. In this article, the author explores the trend towards legislative regulation of the use of digital technologies in public law relations in the field of ecology. Defining the essence of the digital transformation of the named sphere, the author reveals the

characteristic historical and normative stages, the significance of which could form a direction for improving the approach to regulating environmental legal relations. The author comes to the conclusion that the transition to sustainable digitalization is designed to optimize and improve the mechanism of public administration in the field of ecology, including identifying the effectiveness and complexity of its legal implementation.

Keywords: Digital transformation, Ecology, Environmental legal relations, Digitalization, Public law relations, Constitutional and legal arrangement, Environmental protection

Направленность политико-правового курса государства оказывает колоссальное влияние на структуру отношений с обществом в различных сферах. В последнее десятилетие в России усиливается тенденция к законодательному регулированию использования цифровых технологий в публично-правовых отношениях, том числе в сфере экологии.

Исследуя сущность цифровой трансформации названной сферы, важно выявить характерные историко-нормативные этапы, значение которых могло определить направление к совершенствованию подхода регулирования экологических правоотношений. Так, впервые за всю историю нашей страны законодательное закрепление направления охраны природы произошло в начале XX столетия — в 1929 году в резолюции Первого Всероссийского съезда по охране природы [1. С. 386–402]. Безусловно, в этот временной период вопросы перехода к цифровизации сфер общества широко не рассматривались, однако цель конституционно-правового обустройства экологии преследовала одновременное повышение материального и культурного уровня жизни людей. Иными словами, «надлежащее качество окружающей человека природной среды признается элементом материального благосостояния людей» [2. С. 80].

Советское природоохранное законодательство, основанное на Конституции Союза Советских Социалистических Республик 1936 года (далее – Конституция 1936 года) [3. С. 3], «развивалось по пути установления универсальных правовых норм охраны природы и формирования отраслей, специализированных применительно к основным природным объектам – земле, ее недрам, водам, лесам и животному миру» [2. С. 80]. Более того, представляется важным отметить значимость в исследуемой тематике статей 4, 6, 10, 11 и 131 Конституции 1936 года, в которых закреплены «основы народного хозяйства, государственная собственность на главные природные объекты..., основные начала социалистического планирования экономики» [2. С. 190], принцип охраны личной собственности граждан и общая обязанность советских граждан беречь и охранять природные объекты. Вышеизложенные общие принципиальные положения в совокупности и образуют исторический подход к правовому регулированию охраны окружающей природной среды в названный период времени существования нашего государства.

К следующему значимому для исследования сущности цифровой трансформации сферы экологии историческому этапу конституционно-правового обустройства нашей страны следует отнести принятие Конституции Союза Советских Социалистических Республик в 1977 году (далее – Конституция 1977 года) [3. С. 3],

на котором в отличие от Конституции 1936 года закреплена природоохранительная функция социалистического государства. В частности, Конституция 1977 года утвердила «социалистическую концепцию бережного отношения общества развитого социализма к окружающей его природной среде» [2. С. 190], в которой государственному аппарату отводится решающая роль. Так, в статье 18 Конституции 1977 года установлено, что «в интересах настоящего и будущих поколений в СССР принимаются необходимые меры для охраны и научно обоснованного, рационального использования земли и ее недр, водных ресурсов, растительного и животного мира, для сохранения в чистоте воздуха и воды, обеспечения воспроизводства природных богатств и улучшения окружающей человека среды» [5. С. 15]. По смыслу статей 11 и 10 Конституции 1977 года государство обязано охранять социалистическую собственность, в том числе землю, ее недра, воды, леса, и создавать условия для ее преумножения [5. С. 15].

Правореализационный механизм природоохранительной функции советского государства предусматривался статьями 73, 131 и 147 Конституции 1977 года. Стоит отметить, что по истечении определенного времени эффективность правореализационного механизма природоохранительной функции советского государства, при наличии отдельных недостатков, оценивалась учеными юристами-экологами весьма положительно [2. С. 193].

Представляется, что в рассмотренных историко-нормативных этапах публично-правовые отношения в сфере экологии хоть прямо и не содержали упоминание об использовании цифровизации, но в сравнении с современностью отражали некоторые задачи цифровой трансформации экологии и природопользования.

Сущность цифровой трансформации сферы экологии тесно связана с современным историко-нормативным этапом конституционно-правового обустройства нашей страны, который берет отсчет с Конституции Российской Федерации 1993 года (далее – Конституция 1993 года) [6. С. 1], где закреплены задачи экологии как в экономической, так и социальной сферах страны. Выделяют группу норм Конституции 1993 года, которая целенаправленно посвящена регулированию экологических правоотношений.

Так, статья 9 Конституции 1993 года устанавливает, что земля и другие природные ресурсы используются и охраняются в Российской Федерации как основа жизни и деятельности народов, проживающих на соответствующей территории, а также то, что земля и другие природные ресурсы могут находиться в частной, государственной, муниципальной и иных формах собственности [6. С. 7].

Более того, согласно статье 36 Конституции Российской Федерации 1993 года устанавливается, что:

- граждане и их объединения вправе иметь в частной собственности землю;
- владение, пользование и распоряжение землей и другими природными ресурсами осуществляются их собственниками свободно, если это не наносит ущерба окружающей среде и не нарушает прав и законных интересов иных лиц;
- условия и порядок пользования землей определяются на основе федерального закона» [6. С. 15].

Статья 42 Конституции 1993 года регламентирует, что каждый имеет право на благоприятную окружающую среду, достоверную информацию о ее состоянии и на возмещение ущерба, причиненного его здоровью или имуществу экологическим правонарушением» [6. С. 18]. При этом статья 58 Конституции 1993 года устанавливает, что «каждый обязан сохранять природу и окружающую среду, бережно относиться к природным богатствам» [6. С. 21].

Однако, не смотря на такую достаточно категоричную конституционно-правовую регламентацию обустройства экологической сферы современной России, повсеместно констатируется деэкологизация, а также иные отступления от концептуальных эколого-конституционных постулатов в различных отраслях российского права. Представляется, что «основной причиной ослабления...реализации сформулированных положений ... является объективное противоборство экономики и экологии, усиленное эгоизмом свободного рынка товаров, финансов и услуг» [7. С. 292].

Таким образом, в сложившейся правовой реалии переход к устойчивой цифровизации призван оптимизировать и усовершенствовать механизм государственного управления в сфере экологии, в том числе выявить результативность и комплексность ее правореализации. В этой связи рассмотрим актуальные эколого-правовые документы стратегического планирования.

Во-первых, Указом Президента Российской Федерации от 21 июля 2020 № 474 [9] обозначены отечественные пути развития до 2030 года, в числе которых определена цифровая трансформация: «...в целях осуществления прорывного развития Российской Федерации, увеличения численности населения страны, повышения уровня жизни граждан, создания комфортных условий для их проживания, а также раскрытия таланта каждого человека постановляю:...определить следующие национальные цели развития Российской Федерации...д) цифровая трансформация...» [9].

Далее, Распоряжением Правительства Российской Федерации от 8 декабря 2021 года № 3496-р [8] (далее – Распоряжение от 8 декабря 2021 года) в сфере экологии и природопользования определены технологические инструменты цифровой трансформации. К ним относятся: «искусственный интеллект; дистанционное зондирование Земли; беспилотный летательный аппарат; технология интернет вещей; большие данные; аналитическая обработка данных; цифровой двойник» [8].

Исследование нормативного регулирования вышеприведенных технологических инструментов цифровой трансформации позволило заключить, что создание и внедрение их в России будут способствовать совершенствованию публично-правовых экологических отношений. Например, «технологии больших данных и аналитической обработки данных будут использоваться в рамках развития отрасли экологии и природопользования для накопления, хранения, анализа и обработки данных в создаваемых федеральных государственных информационных системах и цифровых платформах» [8].

Весьма детально в Распоряжении от 8 декабря 2021 года определяется механизм цифровой трансформации в сфере охраны окружающей среды, реализация которого позволит оптимально и оперативно совершенствовать подход к регулированию экологических правоотношений: «формирование и развитие цифровой платформы

услуг мониторинга состояния окружающей среды, обеспечивающей управление природоохранной деятельностью и экологической безопасностью;...обеспечение интеграции с существующими и разрабатываемыми государственными информационными системами для функционирования тематических информационных систем и обмен данными между этими информационными системами и ресурсами в рамках задач отрасли экологии и природопользования;...комплексный перевод процессов оказания государственных услуг и функций в цифровой вид» [8].

Таким образом, следует резюмировать, что создание благонадежных условий цифровой трансформации, своевременность и качество (с учётом историко-нормативного опыта) решения появившихся в связи с этим проблем и вызовов, минимизация политических и правовых рисков позволят последовательно и эффективно перейти к устойчивой цифровой трансформации публично-правовых отношений в сфере экологии.

Список литературы

1. Всероссийский съезд по охране природы (1; 1929; Москва). Труды 1-го Всероссийского съезда по охране природы / под ред. М. П. Потемкина, Б. П. Дитмара и С. А. Северцова; Всерос. о-во охраны природы. Главнаука. Москва: Всерос. о-во охраны природы, 1930 (типо-лит. им. т. Воровского). 222, [2] с.; 21X15 см. (Всероссийское общество охраны природы. Главнаука).
2. Колбасов О. С. Избранное. Теория экологического / И. О. Краснова, Г. А. Мисник и др.; отв. ред. И. О. Краснова. М.: РГУП, 2017. +CD-ROM. С. 80.
3. Конституция Союза Советских Социалистических Республик 1936 года. URL: <https://docs.cntd.ru/document/901941395> (дата обращения: 18.09.2022).
4. Конституция Союза Советских Социалистических Республик 1977 года. URL: <https://docs.cntd.ru/document/901817660> (дата обращения: 18.09.2022).
5. Конституция Союза Советских Социалистических Республик 1977 года. URL: <http://www.hist.msu.ru/ER/Etext/cnst1977.htm> (дата обращения: 18.09.2022).
6. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Официальный текст с внесенными поправками от 14.03.2020 опубликован на официальном интернет-портале правовой информации. URL: <http://www.pravo.gov.ru> (дата обращения: 04.07.2020).
7. Нижник Л. С. Перспективы реализации новых положений Конституции Российской Федерации в сфере экологии // Новеллы Конституции Российской Федерации и задачи юридической науки. Материалы конференций: в 5 ч. XVIII Международная научно-практическая конференция (Кутафинские чтения) Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) и XXI Ежегодная международная научно-практическая конференция юридического факультета Московского государственного университета имени М. В. Ломоносова (МГУ) в рамках X Московской юридической недели. Москва, 2021. С. 291–293.
8. Распоряжение Правительства Российской Федерации от 08.12.2021 № 3496-р «Об утверждении стратегического направления в области цифровой трансформации

отрасли экологии и природопользования» // Собрание законодательства Российской Федерации, 20.12.2021, № 51, ст. 8889.

9. Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» // «Российская газета», № 159, 22 июля 2020 г.

А. М. Нобатов,
старший преподаватель, кафедра цифровой экономики,
Туркменский государственный институт экономики и управления
А. И. Маткаримов,
преподаватель, кафедра цифровой экономики,
Туркменский государственный институт экономики и управления

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ В ЗАЩИТЕ КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ЭКСПЛОЙТОВ

Аннотация. В данной работе рассмотрены вопросы развития систем защиты компьютерных сетей от эксплойтов, создания цифровой базы защитных протоколов и развития технологий защиты компьютерных сетей. С помощью методов системного анализа проведено исследование развития цифровых технологий в области защиты данных и сетей. Даны рекомендации по внедрению технологий в отрасль системной защиты данных в Интернете.

Ключевые слова: цифровая экономика, компьютер, технологии

PRIORITY AREAS IN PROTECTION OF COMPUTER SYSTEMS AND AGAINST EXPLOITS

Abstract. In this paper, the issue of developing systems for protecting computer networks from exploits, creating a digital database of security protocols and developing technologies for protecting computer networks was considered. A systematic and analytical analysis of the development of digital technologies in the field of data and network protection was carried out. Recommendations are given on the introduction of technologies in the field of system data protection on the Internet.

Keywords: Digital economy, Computer, Technology

С растущими потоками программ-вымогателей, съедающих большую часть новостных лент, мы знакомимся и с новым сопутствующим вредоносным ПО: эксплойтами. Несмотря на то, что они разные, могут, по-видимому, сопровождать приложения и вызывать риски (угроза, с которой вы только что столкнулись, или поведение, которое вы можете наблюдать в своей системе). Эксплуатируемая машина может быть не заражена, но ее можно использовать для воздействия или заражения каждой машины в вашей среде, если уязвимости в сети не контролируются должным образом [1. С. 237].

Что же такое эксплойт?

Эксплойт – это уязвимость базового приложения, реализации приложения, ОС или другого аспекта самой машины, которая может повлиять на систему

и сделать ее уязвимой. Кратко говоря, это слабость, которая используется против вас. Следующее должно помочь согласовать, где эти элементы вписываются в топографию атаки:

1. Уязвимость – слабость в части вашей вычислительной инфраструктуры.
2. Риск – это то, что возникает из-за существующей уязвимости, и его можно уменьшить, принять или проигнорировать в зависимости от возможности его использования.
3. Эксплойт использует уязвимость и таким образом заставляет бизнес страдать от уязвимости из-за использования эксплойта [2. С. 310].

Существуют эксплойты системного уровня и уровня приложений, которые можно использовать против машины. Например, эксплойт системного уровня может обойти службу RPCSS через атаку переполнения буфера на машинах под управлением английской версии Windows 2K, Windows 2003 и Windows NT 4.0 SP3–6a. Имея в виду машины, работающие под управлением этих версий ОС, служба RPCSS имеет уязвимость, которая позволяет командам превысить выделение памяти для этого процесса и вставлять команды для выполнения в другом пространстве памяти [3. С. 78].

Слабый код обнаруживается с помощью эксплойтов приложений путем проверки исходного кода на наличие уязвимых библиотек или с использованием таких методов, как фаззинг. Фаззинг – это полуавтоматический или автоматический метод тестирования, который берет случайные или недопустимые данные и пропускает их через входные данные приложения, проверяя его на наличие неожиданных сбоев или возможных утечки памяти и переполнения буфера. Несколько недавних атак были нацелены на Java-приложения. Каждый раз, когда вы нажимаете на приглашение «обновить Java», чтобы его игнорировать, вы открываете себя для того, чтобы приложение Java использовалось неизвестными злоумышленниками. Многие продвинутые атаки, связанные с наборами эксплойтов, основаны на этом методе. Нажав на сайт, на который влияет ЕК, например сайт Совета ЕС, вы передаете информацию о вашей низкоуровневой Java на их серверы, позволяя им отправить зашифрованный пакет на машину. Это, в свою очередь, позволит обойти функцию безопасности Java, передав ключи вашего компьютера злоумышленнику [4. С. 280].

Кратко говоря, эксплойт – это дыра в вашей броне, которую используют против вас. Уязвимость – это дыра, и риск заключается в том, что она будет раскрыта.

Как же защитить свои компьютеры от эксплойтов? Необходимо установить какое-то приложение? На деле все не так просто. Большая часть предотвращения таких атак, использующих ваши системы, заключается в знании вашей среды и контроле над ней. Существует множество технических средств контроля, которые можно применить к вашим системам, чтобы предотвратить их использование из-за уязвимостей:

1. Управление исправлениями. Самый простой способ заполнить дыру в безопасности – убрать ее. Знание того, что вы исправляете, является ключевым, так как вы не хотите снимать всю сеть. [5. С. 64].

Регулярное применение исправлений помогает предотвратить проблемы и снизить риск заражения за счет устранения уязвимостей, которые могут привести к эксплуатации. Такие элементы, как приложения Java, Flash, Adobe и Microsoft, включая операционную систему, необходимо регулярно обновлять. Это можно сделать с помощью служб Центра обновления Windows с сервера MS или другого

стороннего приложения. Для систем UNIX/Linux вы можете использовать Chef, Puppet или сторонний инструмент, например Lumension.

2. Оцените свои исправления по тому, насколько они важны для бизнеса и операций.

a) если элемент не может быть исправлен, то бизнес должен принять на себя риск эксплуатации;

b) имейте план возврата на случай, если патч что-то сломает. Вы всегда будете спать спокойнее, если действие можно будет отменить в вашем окружении.

3. Вывод из эксплуатации старых устаревших систем – у некоторых все еще работают устаревшие приложения, для запуска которых требуется сервер Windows 2000; однако даже наличие ОС, уязвимой в инфраструктуре, не очень хорошо, особенно если вы повторно используете пароли (как это делают многие). Получение доступа к этой машине может нанести ущерб, поскольку пароли могут быть сброшены, а доступ к файловой системе может использоваться, если есть какие-либо подключенные диски [5, С. 64].

4. Установите приложения безопасности на конечных точках для защиты от эксплуатации на уровне сети и системы.

a) продукт безопасности с решением IDS/IPS предотвратит использование трафика, например, при атаке MITM (человек посередине) или перенаправлении DNS;

b) наличие антивирусного приложения любого типа обычно останавливает многие попытки эксплуатации приложения с помощью вредоносного исполняемого кода, сканирования запутанного кода или его идентификации после того, как код будет раскрыт во время выполнения.

Предотвращение эксплуатации ваших систем требует планирования и настройки, чтобы гарантировать, что установка исправлений пройдет гладко и не приведет к непредвиденному падению некоторых аспектов среды. Пользователям рекомендовано использование систем безопасности ESET или любой другой системы, в которую включен блокировщик эксплойтов. Технология блокировки эксплойтов в приложениях ESET отслеживает существующие приложения и компоненты Microsoft, гарантируя отсутствие злонамеренного поведения. Если обнаружение срабатывает из-за подозрительного поведения приложения, угроза немедленно блокируется с помощью информации, отправляемой в системы Live Grid, чтобы остановить атаку на другие системы по всему миру [6. С. 176].

Список литературы

1. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации: учебное пособие. М.: Риор, 2018. 400 с.
2. Бирюков А. А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2019. 478 с.
3. Глинская Е. В., Чичварин Н. В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие. М.: Инфра-М, 2019. 78 с.
4. Информационная безопасность открытых систем: в 2 т. Т. 2: Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. М.: ГЛТ, 2008. 558 с.

5. Кузнецова А. В. Искусственный интеллект и информационная безопасность общества / А. В. Кузнецова, С. И. Самыгин, М. В. Радионов. М.: Русайнс, 2017. 64 с.
6. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: учебное пособие для вузов. М.: Горячая линия – Телеком, 2019. 320 с.

Б. К. Оразов,
старший преподаватель,
заведующий кафедрой цифровой экономики,
Туркменский государственный институт экономики и управления

ОСОБЕННОСТИ РАЗВИТИЯ ЧЕЛОВЕЧЕСКОГО КАПИТАЛА В ЦИФРОВОЙ ЭКОНОМИКЕ

Аннотация. В данной работе рассмотрен вопрос развития человеческого капитала в периоды развития цифровых технологий и цифровой экономики, методы оценки человеческого потенциала и создания новых условий работы в технологичный период развития. Проведен системный анализ развития человеческого капитала и его влияние на внедрение инноваций. Даны рекомендации по внедрению технологий в отрасль.

Ключевые слова: цифровая экономика, человеческий потенциал, технологии

FEATURES OF THE DEVELOPMENT OF HUMAN CAPITAL IN THE DIGITAL ECONOMY

Abstract. In this paper, the issue of the development of human capital during the periods of development of digital technologies and the digital economy, methods for assessing human potential and creating new working conditions in the technological period of development were considered. A systematic and analytical analysis of the development of human capital and its impact on the introduction of innovations has been carried out. Recommendations are given for the introduction of technologies in the industry.

Keywords: Digital economy, Human potential, Technologies

2000-е гг. ознаменовали собой бурное развитие цифровых технологий и их эффективное внедрение во всех сферах экономики. Как показывает мировой опыт, реализация экономических отношений в цифровой среде позволила повысить уровень жизни населения страны, обеспечить устойчивое развитие и диверсификацию экономики [1. С. 237].

Важно отметить, что цифровизация создает на рынке труда новые рабочие места, а также новые возможности для реализации творческого потенциала. Эти тенденции, в свою очередь, изменяют методы работы, принципы, цели и содержание системы образования. Цифровая система образования – это индивидуализированная, географически независимая система образования, предназначенная для развития необходимых навыков, получения теоретических знаний, удовлетворения потребностей обучающихся. Переход к персонифицированному (т. е. полностью адаптированному к каждому отдельному обучающемуся) методу обучения приво-

дит к повышению гибкости системы образования, способствует полной адаптации предоставляемого образования к возможностям, уровню знаний, желанию и целям обучающихся [2. С. 130].

Основной целью системы образования в условиях цифровой экономики является создание информационного пространства знаний. Основным инструментом развития системы образования с помощью информационно-коммуникационных технологий является создание различных технологических платформ, позволяющих осуществлять дистанционное обучение. Для выполнения этих задач необходимо постоянное обновление информационно-коммуникационной базы образовательных учреждений, обеспечение интерактивными компьютерными технологиями, использование интеллектуальных технологий в воспитательной работе, создание цифровых площадок для проведения дистанционного обучения, внедрение цифровых систем управления обучением, создание единой базы данных учащихся, оцифровка учебно-методической информации. Будущее высшего образования – за виртуальными лабораториями и технологиями дополненной реальности, 3D-моделированием и робототехникой, искусственным интеллектом, нейронными сетями, мобильными и облачными технологиями, массовыми открытыми онлайн-курсами и другими, связанными с использованием инновационных технологий. Развитие технологий, их разнообразие и доступность побуждают педагогов к творческой работе, помогают использовать новые способы работы с учащимися по основным принципам классического образования [3. С. 450].

Выстраивание экономических отношений в цифровой среде, развитие цифровых навыков участников этого процесса является важным вопросом. Повышение доступности Интернета и снижение стоимости его услуг открывают новые возможности для организации образовательных услуг. Технологии онлайн-образования послужат гибкой технологической базой непрерывного образования граждан, формирования деловых навыков в соответствии с современными требованиями [4. С. 182].

Появление цифровых технологий и услуг в нашей повседневной жизни может уменьшить зависимость людей от географического положения. Цифровизация также позволяет лицам, ищущим работу, получить доступ к своим возможностям трудоустройства через современные цифровые порталы с доступом к обширной базе данных о поиске работы и имеющихся вакансиях. Ускоряется процесс поиска и устройства на работу [5. С. 210].

В современном мире информационно-коммуникационные технологии призваны удовлетворять все возрастающие потребности экономики и общества в телекоммуникационных услугах, и ее развитие во многом ориентировано на освоение информационных технологий и совершенствование инфраструктуры приема и отправки информации. Развитие услуг информационно-коммуникационных технологий открывает широкий путь к созданию в стране информационного общества, повышению эффективности информационного общения граждан, бизнеса и государства. Сегодняшняя развитая система Интернета определяет темпы развития экономики стран мира, конкурентоспособность отраслей народного хозяйства, состояние людей [6. С. 530].

Новые технологии позволяют работать удаленно, что позволяет повысить эффективность найма специалистов в регионах. Технологии автоматизируют

рабочие места и в то же время создают новые рабочие места и новые способы получения дохода в традиционных отраслях. Цифровые технологии позволяют сократить время общения и ускорить все бизнес-процессы, поэтому основное внимание уделяется интеллектуальному богатству человека. На предприятиях, которые повысят их конкурентоспособность на рынке, перед внедрением новой техники и технологий выдвигаются новые способы управления и организации работников предприятия, изменение кадровой политики, подготовка компетентных работников, преобразование системы управления персоналом предприятия [7. С. 304].

Человеческий капитал является важнейшим условием обеспечения цифрового развития экономики и перехода на инновационный путь развития с широким использованием цифровых технологий. Цифровые технологии в экономике создают новые вызовы для работодателей и бизнеса в их бизнес-процессах. Модернизация и обновление технологий тесно связаны с развитием человеческого капитала. Основной задачей государственного сектора является повышение производительности труда, увеличение добавленной стоимости и повышение рентабельности. Наличие глобальной конкуренции создает новые условия в обрабатывающей промышленности, которые зависят от взаимосвязанных вопросов и факторов – работодателя и человеческого капитала. Цифровая экономика ставит перед системой образования важные задачи, такие как освоение новых дополнительных знаний, навыков и умений.

Развитие цифрового образования является необходимым условием развития цифровой экономики в целом, так как способствует развитию человеческого капитала, составляющего основу цифровой экономики.

Список литературы

1. Абляев, С. В. Управление человеческими ресурсами на основе компьютерных технологий. Москва: Финансы и статистика, 2019. 176 с.
2. Алавердов А. Р. Управление человеческими ресурсами организации: учебник. Москва: МФПУ Синергия, 2019. 656 с.
3. Асалиев А. М. Экономика и управление человеческими ресурсами: учебное пособие / А. М. Асалиев, Г. Г. Вукович, Т. Г. Строителева. Москва: Инфра-М, 2018. 240 с.
4. Бирман Л. Управление человеческими ресурсами. Москва: ИД «Дело» РАНХиГС, 2022. – 346 с.
5. Веснин В. Р. Управление человеческими ресурсами. Теория и практика: учебник. Москва: Проспект, 2013. 688 с.
6. Генкин Б. М. Управление человеческими ресурсами: учебник / Б. М. Генкин, И. А. Никитина. Москва: Норма, НИЦ Инфра-М, 2013. 464 с.
7. Управление человеческими ресурсами: учебное пособие / под ред. А. М. Руденко. Ростов на Дону: Феникс, 2018. 320 с.

А. А. Петров,

доктор экономических наук, профессор,
Московский государственный юридический
университет имени О. Е. Кутафина, академик,
Российская академия естественных наук

ВОСПРОИЗВОДСТВО ОТЕЧЕСТВЕННОЙ ИТ-ИНДУСТРИИ В УСЛОВИЯХ САНКЦИЙ

Аннотация. В работе анализируется состояние отечественной ИТ-индустрии, последствия ухода зарубежных ИТ-компаний из России. Показана угроза, нависшая над российской ИТ-отраслью и экономикой в связи со сменой иностранными ИТ-компаниями своей юрисдикции. Проанализирована эволюция государственной поддержки ИТ-индустрии.

Ключевые слова: ИТ-рынок, ИТ-специалист, ИТ-индустрия, «утечка мозгов», фрилансер, правительственная поддержка, кибербезопасность, национальная безопасность, технологическая изоляция.

REPRODUCTION OF THE DOMESTIC IT-INDUSTRY IN THE CONDITIONS OF SANCTIONS

Annotation. The paper analyzes the state of the domestic IT-industry, the consequences of the departure of foreign IT-companies from Russia. The threat looming over the Russian IT-industry and economy in connection with the change of jurisdiction by foreign IT-companies is shown. The evolution of government support for the IT-industry is analyzed.

Keywords: IT-market, IT-specialist, IT-industry, «Brain drain», Freelancer, government support, Cyber security, National security, Technological isolation.

Введение. Социальный прогресс на основе экономического роста, обеспечиваемый развитием науки и инновационными технологиями, и конкурентные преимущества на глобальном рынке определяются способностью увидеть новые тренды развития и эффективностью управления научно-технологическим развитием. Ядром современного прогресса выступают цифровые технологии и связанные с ними производства.

Стартовавшая на рубеже двух столетий, Четвертая промышленная революция (ЧПР) набирает обороты. Информационно-технологические технологии интенсивно пронизывают всю систему национальных и международных отношений, определяя гонку на опережение между странами. В этой технологической гонке уже сформировались лидеры и догоняющие. Лидеры, имеющие мощную собственную материально-финансовую и научно-техническую базу и мощнейшую государственную финансовую и законодательную поддержку, значительно опережают догоняющих. Сократить образовавшийся разрыв требует значительных частных усилий и еще более мощной правовой и финансовой поддержки государства. Именно благодаря участию и поддержке государства китайские ИТ-корпорации

ворвались в группу лидеров и фактически возглавили внедрение и использование широкополосного доступа к сети 5G WiFi, разработки и применение искусственного интеллекта (ИИ) и сильные позиции в области информационных технологий (в области информационно-аппаратного оборудования). Успехи в ИТ-сфере активно продвигаются в Китае в экономической и социальной сферах. В частности, власть успешно контролирует китайскую область интернета. Тем не менее Китаю не удастся существенно ущемить интересы американских программно-компьютерных гигантов, которые с государственной поддержкой первыми освоили мировой ИТ-рынок.

Базу ИТ-бизнеса США составляют хорошо известные российскому деловому и потребительскому сообществу крупнейшие международные американские онлайн корпорации: Google, Meta (признана экстремистской организацией, а ее деятельность на территории Российской Федерации запрещена), Amazon, Apple, Microsoft.

Частная американская операционная система Windows ИТ-гиганта Microsoft стала международным стандартом. На этой операционной системе работают не менее 95% всех компьютеров мира. Отказаться от нее, заменить ее ни в ближайшей, ни в отдаленной перспективе не представляется возможным.

Россия после развала Советского Союза стремительно вклинилась в мировую интеграцию на условиях сформированной небольшой группой развитых стран системы международного разделения труда и системы международных экономических отношений, в основе которой был заложен неокOLONиальный подход. Этот интеграционный прыжок был сделан без учета сохранения национального суверенитета, а также без учета национальной и экономической безопасности государства. В обмен на потерю национального суверенитета Россия получила зарубежную технологию, иностранное оборудование, потребительские товары и продовольствие и программно-аппаратное оборудование из-за рубежа, главным образом из США и стран Евросоюза. Надо подчеркнуть, все импортное оборудование и технологии были для России прогрессивными, но устаревшими для стран-производителей и экспортеров. Такая интеграция в мирохозяйственные связи стала и кнутом, и пряником для сдерживания и управления Россией, когда она пыталась выйти с установленного для нее и контролируемого извне пути.

Западные санкции становятся для России стимулом преобразования национальной экономики, формирования должной ее структуры, гарантирующей национальную и экономическую безопасность и национальный суверенитет принятия решений. Санкции выступают катализатором воссоздания и развития отечественной ИТ-индустрии и электроники и прежде всего в секторах экономики, требующих обеспечения национальной цифровой инфраструктурной безопасности. Санкции заставили Россию переходить на использование отечественного ПО. В 2016 г. начал функционировать отечественный реестр ПО, который уже сегодня насчитывает почти 13 тыс. программных продуктов по всем классам ПО. Сегодня Россия может заменить иностранные программные продукты на отечественные. И все же зависимость от зарубежных решений остается достаточно высокой. В частности, остается открытой проблема критической информационной

инфраструктуры (КИИ), включающей информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети и интегрирующие сети электросвязи.

Россия стала лидером по количеству введенных против нее и ее граждан санкций. На середину 2022 г. общее количество введенных против России с 2014 г. санкций приблизилось к 11 тыс. [6]. В это число входит 1600 экономических санкций [5], устанавливающих торговую, финансовую и технологическую изоляцию России. Такого количества жестких ограничений еще не вводилось никогда. Их цель не только изолировать Россию, но и лишить ее полного национального суверенитета.

Технологическая изоляция разрушает существующие экономические, технологические, социальные, логистические, торговые и культурные связи, нарушает межгосударственное общение, что ударяет по всем странам и экономикам без исключения. Современный мир развивается на постоянно растущей густой сети связей (коммуникаций) и этот процесс усиливается с переходом к цифровой экономике. Межстрановое общение, торговля как встреча цивилизацией позволяют глубже понять культуру, традиции, обычаи, менталитет других народов. На восстановление разрыва этих связей уйдут годы, а возможно и десятилетия.

Государственное финансирование ИТ-отрасль из средств федерального бюджета не должно быть главным, ключевым финансовым источником поддержки и развития ИТ-отрасли. Базовым источником финансирования должны быть частные инвестиции и самофинансирование. Крупные корпорации, имеющие в своей структуре ИТ-подразделения, часть прибыли направляют на развитие ИТ-деятельности, но они не отвечают требованиям для получения преференций. Большая часть ИТ-отрасли представлена предприятиями МСП. Льготы должны доходить до них. Частный предприниматель, вложив свои и/или заемные средства, будет стремиться окупить эти вложения и получить прибыль. Следовательно, надо углубить и расширить условия для частного инвестирования. В частности, освободить от налогообложения ту часть прибыли компании, которая направляется на финансирование ИТ-сферы независимо от сферы деятельности компании.

Индустрия информационных технологий (ИТ-индустрия). ИТ-индустрия основывается на использовании компьютеров, программного обеспечения, соцсетей и ИТ-инфраструктуры, обеспечивая передачу и управление информацией, что имеет ключевое/коренное/фундаментальное значение для общества, государства и организаций/компаний. ИТ-индустрия является важнейшим средством/инструментом механизма государственного управления, системы управления общественной жизнью, рыночного механизма управления предпринимательской деятельностью.

Индустрия информационных технологий (ИТ-индустрия) развивается на трех китах: 1) специалисты – разработчики программ, производители компьютерного оборудования, ИТ-интеграторы, продвигающие ИТ-продукцию на рынок, 2) информационные технологии, включая программные средства и организационно-методическое обеспечение, 3) компьютерное оборудование.

Взаимодействие двух ведомств. Сложность понимания взаимодействия кроется в существующей системе управления, которая должна согласовать интересы

разных ведомств: куратором радиоэлектронной отрасли выступает Минпромторг, тогда как все разработки программного обеспечения находятся в ведомстве Министерства цифрового развития, связи массовых коммуникаций (Минцифры). Каждое ведомство имеет собственные цели и задачи и собственный реестр аккредитованных компаний в соответствии с кодами Общероссийского классификатора видов экономической деятельности (ОКВЭД). Желательно, согласовать реестры двух ведомств, чтобы программисты видели, какое железо им нужно, а производители железа понимали, что надо производить для того или иного программного обеспечения.

Разработчики железа и программ должны действовать совместно. Необходимо их объединение под единой управленческой «крышей». Нужен механизм согласования интересов обоих ведомств. Его всесторонняя и основательная разработка требует времени. Правительство шаг за шагом формирует подобный механизм. Первым шагом стало решение правительства, обязывающее Минпромторг и Минцифры согласовывать все мероприятия по регулированию госзакупок программного обеспечения и компьютерного оборудования (Постановлением правительства № 1168 от 30.06.2022). Следующим шагом объединения целей и задач обоих министерств стало создание программно-аппаратных платформ отечественной разработки. Следующим шагом должно стать создание единого реестра аккредитованных компаний-производителей электронного оборудования и ИТ-компаний.

Интеграция в мирохозяйственные связи и национальная безопасность. Вхождение в мирохозяйственные связи открыло российский внутренний рынок для зарубежных компаний, включая ИТ-гигантов, которые развернули масштабную деятельность в стране по обслуживанию интересов пришедших в Россию торгового-промышленных компаний. Вместе с ними в страну пришли многочисленное и разнообразное программное обеспечение, индивидуальные компьютеры, ноутбуки, планшеты, смартфоны. Одновременно стал расти спрос на компьютерные программы и ИТ-специалистов. Развитие экономики, управления и общества приобретало цифровую направленность, но в пределах, обеспечивающих потребности зарубежных компаний.

По данным Минцифры в 2020 г. наиболее значимый вклад в развитие российской экономики ИТ-отрасль внесла в торговлю – 13,1%, операции с недвижимостью – 10,5%, добычу полезных ископаемых – 9,8%, госуправление – 8,3%, транспорт и хранение – 6,5%, строительство – 5,7%, финансовый сектор – 4,9% [2].

Средний показатель (8,4%), как и остальные показатели вклада ИТ-индустрии в развитие экономики мизерные и свидетельствуют о уязвимости ИТ-индустрии, о ее неспособности справиться с поставленными задачами. Это подтверждается исследованиями, проведенными специалистами ВШЭ. Согласно полученным результатам, зависимость от зарубежных цифровых решений достигла в 2021 г. 70 % по ПО и ИТ-оборудованию, что обернулось острым дефицитом на российском рынке ИТ-индустрии после ухода иностранных ИТ-компаний [4].

Этот вклад был сделан в основном на базе импортного программно-аппаратного обеспечения. Растущее значение информационных технологий в социальном и экономическом развитии общества, включая процесс цифровизации заставило

власть уделить ИТ-индустрии повышенное внимание. ИТ-индустрия в соответствии с Конституцией страны относится к приоритетным видам деятельности, контролируемым и регулируемым государством.

Санкции коллективного запада еще раз показали ошибочную ставку на безоглядную интеграцию в мировую систему. Интеграция должна вестись с учетом гарантии национальной, информационной и экономической безопасности государства на базе разработок отечественных операционных систем и развития в стране собственного программного и аппаратного обеспечения. России требуются операционные системы с ядрами, полностью разработанными на территории России. Иначе страна окажется в положении догоняющего. Требуются новые разработки, а не доработки зарубежных информационных технологий и компьютерного оборудования.

Нужны критерии, устанавливающие верхние и нижние границы суверенитета и безопасности. Эти показатели следует установить с учетом нестабильности международных отношений, нарушения торгово-экономических и научно-технических договоров, преследования «партнерами» исключительно своих интересов в ущерб другой стороне и возникновения любой форс-мажорной ситуации. Решение озвученной проблемы требует значительных финансовых вливаний государства и частного сектора при налоговой и правовой поддержке государства.

Технократическое решение проблемы ИТ-отрасли: налоговый маневр или первый пакет налоговых льгот. ИТ-деятельностью занимается множество не входящих в ИТ-отрасль компаний с разными целями и с разными конкретными задачами. ИТ-деятельность ведут 1) ИТ-компании, разрабатывающие программное обеспечение для реализации на рынке; 2) ИТ-интеграторы (системные интеграторы), продвигающие на рынке ПО других (чужих) ИТ-разработчиков; 3) компании-разработчики и производители компьютерного железа; 4) компании-разработчики робототехники; 5) компании, обеспечивающие информационную безопасность; 6) компании-разработчики web-дизайна; 7) компании-разработчики web-рекламы; 8) компании-разработчики 3D-анимации; 9) ИТ-подразделения производственных компаний, обеспечивающие информационную безопасность и продвижение продукции головной компании на рынке; и т.д. На начало 2021 г. в России насчитывалось примерно 108 тыс. организаций, прямо и косвенно связанных с информационными технологиями, из которых 52,7 тыс. организаций непосредственно осуществляли деятельность в области информационных технологий. Каждая компания, каждый специалист претендует на преференции от государства, на государственную поддержку. Эта поддержка была гарантирована Федеральным законом № 265-ФЗ от 31.07.2020. Вводимые с 1 января 2021 г. на основании данного закона налоговые льготы получили неофициальное название «налоговый маневр», составив первый пакет налоговых льгот. Однако содержание пакета носило исключительно налоговый характер и охватывало довольно узкий круг ИТ-компаний – юридических лиц [7]. Налоговый маневр фактически получил технократическую направленность и существенно сузил число компаний ИТ-отрасли, подпадающих под федеральные налоговые льготы. Вступившие в силу с 01.01.2021 льготы не устранили сложности их применения из-за отсутствия необходимых разъяснений

используемых ИТ-терминов: постановка задач, разработка, модификация, адаптация, тестирование, сопровождение и отладка программ ЭВМ. Только спустя девять месяцев в сентябре 2021 г. после вступления в силу ФЗ № 265 Минцифры России разъяснило толкование отдельных понятий в сфере ИТ-деятельности для их применения заинтересованными сторонами [7].

Воспользоваться преимуществами налогового маневра может только та ИТ-компания, которая отвечает установленным требованиям [9], что по сути охватывает только часть организаций ИТ-индустрии, оставив в стороне ИТ-инфраструктуру и ИТ-подразделения крупных компаний с работающими в них десятками и сотнями ИТ-специалистов. При этом налоговый маневр не учитывает социальную направленность. В итоге потребовалась существенная корректировка принятых мер государственной поддержки.

Российская ИТ-миграция и экономика принимающих стран. Отток ИТ-специалистов, даже незначительный символизирует о законодательных и иных трудностях ведения работы в стране, создает вакуум, который заполняется специалистами низшей квалификационной категории. Мгновенный рост численности ИТ-сообщества в принимающих странах за счет российских специалистов позволяет поднять в них ИТ-уровень и как следствие повысить уровень ИТ-обеспечения предпринимательского сообщества. Это рывок в инновационно-технологическом и социально-экономическом развитии принимающих стран.

Успехи стран в освоении цифровой экономики определяются долей ЦЭ в ВВП страны. По данным Бостонской консалтинговой группы (BCG) за 2010-2016 гг. прирост доли цифровой экономики в ВВП России составил 0,9%, тогда как в Великобритании аналогичный показатель составил 4,1 % и в Китае 1,4 %. Доля в ВВП является важным критерием уровня развития цифровой экономики. По этому показателю Россия уступает лидерам в 3-4 раза. Важно отметить, что даже этот мизерный прирост был обеспечен обосновавшимися в России зарубежными ИТ-компаниями.

Таблица 1

Доля цифровой экономики в ВВП в странах G20 [3].

Страна	2010	2016
Великобритания	8,3	12,4
Южная Корея	7,3	8,0
Китай	5,5	6,9
Евросоюз	3,8	5,7
Индия	4,1	5,6
Япония	4,7	5,6
США	4,7	5,4
Мексика	2,5	4,2
Германия	3,0	4,0
Саудовская Аравия	2,2	3,8
Австралия	3,3	3,7

Страна	2010	2016
Канада	3,0	3,6
Италия	2,9	3,5
Франция	2,9	3,4
Аргентина	2,0	3,3
Россия	1,9	2,8
ЮАР	1,9	2,5
Бразилия	2,2	2,4
Турция	1,7	2,3
Индонезия	1,3	1,5

ИТ-индустрия относится к приоритетному направлению технологического развития страны. Универсальный характер информационных технологий открывает им путь во все сферы человеческой деятельности. ИТ-профессия привлекательна с т.з. перспективы, занятости и заработной платы.

Решение о необходимости подготовки кадров для ИТ-индустрии было озвучено в 2017 г. в принятой программе «Цифровая экономика Российской Федерации» (распоряжение Правительства России от 28 июля 2017 г. № 1632-р). Тогда вопрос стоял об обычной рутинной подготовке кадров для зарождающейся цифровой экономики страны, как для любой иной отрасли. В рамках данной программы подготовки ИТ-кадров в период 2019-2024 гг. предполагается наращивать число ИТ-выпускников с 50 тыс. в 2019 г. до 120 тыс. выпускников в 2024 г. [8].

Таблица 2

**Выпуск ИТ-специалистов по программам высшего образования
в сфере информационных технологий**

Год	Число выпускников
2019	50000 чел
2020	60000 чел
2021	80000 чел
2022	90000 чел
2023	100000 чел
2024	120000 чел

Всего за 2019–2024 гг. будет выпущено по данной программе 500 тыс. ИТ-специалистов общего направления. Но каких специалистов готовит высшая школа? Выпускников с фундаментальными знаниями, без конкретной специализации для предпринимателя и без понимания производственных процессов. Этим выпускников потребуется еще 2–3 года доводить до ума на производстве. Фактически специалисты требуемой для предпринимателя квалификации и специализации будут поступать в производство в течение 2022–2027 гг. Часть из этого выпуска уйдет

из профессии, другая часть мигрирует, а спрос за этот период на ИТ-специалистов возрастет. При таких темпах стране не хватит и 20 лет для удовлетворения спроса на ИТ-специалистов.

К тому же в годы разработки и принятия программы именно зарубежные ИТ-компании, работавшие на территории России и набиравшие в свой штат российских ИТ-специалистов, поставляли сетевое оборудование, обеспечивали цифровую инфраструктуру, гарантировали цифровое обеспечение и поставляли все необходимые ИТ-услуги госорганам и российским компаниям.

Вопроса дефицита и утечки ИТ-кадров в прошедшие десятилетия партнерства России с зарубежными ИТ-компаниями не было. Подготовка ИТ-кадров шла в неспешном, рутинном порядке. И тогда никто не хотел замечать и видеть угрозу, которую представляли иностранные ИТ-компании, обслуживавшие интересы госорганов и предпринимателей. Однако пришло ясное понимание, что ключевым тормозом развития отечественных разработок программного обеспечения является острая нехватка отечественных кадров. Постепенно приходило осознание возрастающей зависимости отечественной ИТ-системы от зарубежных ИТ-компаний и вместе с этим обострение угрозы национальной безопасности, если медлить с подготовкой отечественных ИТ-кадров.

Сложившиеся новые экономико-технологические условия потребовали массовой цифровой грамотности и персонализации образования и дали путевку в жизнь ряду проектов подготовки ИТ-кадров на ближайшую, среднюю и далекую перспективу. Партнерство с зарубежными транснациональными высокотехнологическими компаниями не прошло бесследно, мы получили опыт работы и подготовки ИТ-кадров для производства. Этот опыт следует пропустить через национальный менталитет и лучшее внедрить.

С российского рынка ушел крупнейший американский производитель сетевого оборудования компания Cisco, работавшая в России с 1995 г. Интересна практика работы этой американской компании. За тридцать лет работы на российском рынке эта американская транснациональная компания наладила хорошие деловые связи с российским предпринимательским сообществом – с крупнейшими банками, горнодобывающими, промышленными и страховыми компаниями, с сотовыми операторами и учебными организациями в сфере подготовки ИТ-специалистов.

CISCO организовала собственную сеть подготовки ИТ-кадров международного уровня, которая охватывает 165 государств, включая Россию. В образовательной сетевой системе CISCO учится около 1 млн. студентов, в том числе в странах СНГ примерно 10 тыс. человек (2011 г.), из них в России – 7 тыс. человек [1].

В учебном процессе образовательной системы CISCO используется выпускаемое корпорацией собственное сетевое оборудование. Обучение ИТ-специалистов на собственном оборудовании и с использованием программного обеспечения собственной разработки позволяет компании сформировать собственный рынок потребителей. Это продуманная стратегия на будущее, но в то же время она ставит под контроль национальную цифровую инфраструктуру и область ИТ-услуг. Тем более это сетевое оборудование позволяет собирать информацию о его использовании, а также о российских компаниях, применяющих данные программно-аппаратные комплексы.

Образовательная программа CISCO представляет четырехступенчатую систему подготовки ИТ-специалистов, сочетая классический процесс обучения с новейшими технологиями и современным оборудованием (программно-аппаратными комплексами) (студенты работают с реальным оборудованием), что позволяет выпускникам в процессе обучения освоить фундаментальные знания и практические навыки своей профессии и получать наряду с базовыми знаниями/компетенциями практические навыки.

Особенность системы обучения заключается в ее практической ориентированности на базе постоянного обновления.

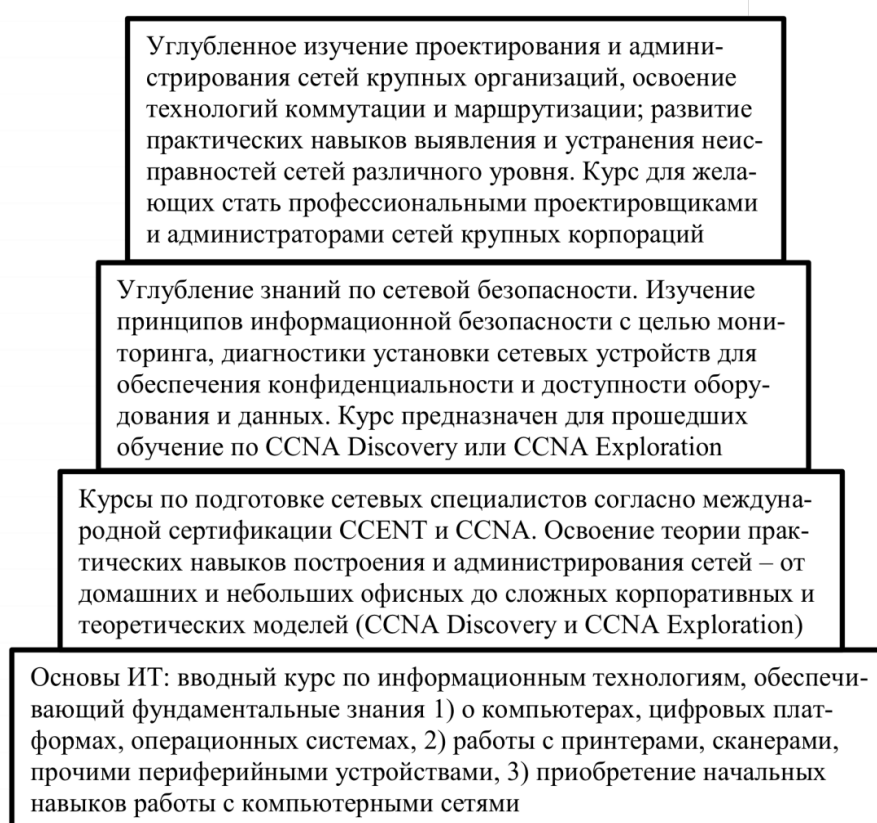


Рис.1. Система CISCO подготовки ИТ-специалистов

Пришло понимание, что сетевое оборудование и ИТ-специалисты представляют единое целое. Необходимо наладить отечественное производство сетевого оборудования на территории России и решить проблему кадрового голода. При этом подготовка ИТ-специалистов должна вестись на отечественном сетевом оборудовании. Дефицит квалифицированных кадров блокирует разработку и внедрение технологических инноваций и сказывается на работе многих ИТ-компаний, которые пытаются решать возникшую проблему через собственные системы наставничества и образовательные проекты с учетом собственной производственной спецификации.

В реальном секторе отечественной экономики требуются ИТ-специалисты, профессионально разбирающиеся как в производственных процессах, так и в высоких технологиях. Это предполагает совместное партнерство вузов и производственных организаций. Здесь надо воспользоваться опытом американской компании CISCO, которая наладила подготовку кадров со школьной скамьи.

Разрабатывая планы на перспективу, компания CISCO, во-первых, наладила партнерско-деловые отношения с учебными заведениями и добилась открытия свыше 50 своих академий при школах, колледжах, вузах; во-вторых, организовала систему обучения и переподготовки преподавателей и работников школ по основам информационных технологий: «Основы ИТ: программное и аппаратное обеспечение ПК». Реализация данных проектов требовала значительных средств. И американская компания выделяла необходимые финансовые ресурсы на эти проекты, поскольку закладывала для себя будущее.

Компания CISCO своей программой информационных технологий охватила как среднее образование, так и высшее. В области высшего образования она активно сотрудничала с МГУ, МГТУ, МФТИ, СПбГУ ИТМО, Сибирским федеральным университетом, Казанским федеральным университетом, Томским политехническим университетом и многими другими. Практически американская компания CISCO окутала своей ИКТ-сетью всю территорию России. Российские компании используют практику американской компании. Примером подобного совместного партнерства является «Академия ИТ», созданная в Нижнем Новгороде «Группой ГАЗ» совместно с учебными заведениями Нижегородской области с учетом перспективно-инновационных задач автомобилестроения. В обучении участвуют сертифицированные преподаватели из ИТ-отрасли, специалисты ИТ-компаний и инженерного центра Горьковского автозавода. Подобные ИТ-школы имеются у Росатома, у группы компаний Иннотех.

Подготовка ИТ-кадров решается в рамках российской системы образования, 1) начиная со школьной скамьи, что позволяет обеспечить воспроизводство ИТ-кадров в отдаленном будущем, 2) в отечественных вузах путем создания «цифровых кафедр», на которых студенты старших курсов могут получить дополнительное цифровое образование к своей профильной специальности, 3) открытия курсов для получения второго цифрового образования с 50%-ной компенсацией за счет бюджета. На данный момент действует довольно много программ подготовки ИТ-кадров на все три периода.

Уже сейчас существующие тренды ЦЭ сформировали атлас новых ИТ-профессий, который к 2030 г. выдвинет не меньше 200 новых профессий: клинический биоинформатик, проектировщик нейроинтерфейсов, системный биотехнолог, киберследователь, ИТ-медик, тестировщик и автотестировщик, разработчик систем микрогенерации, строитель «умных» дорог, кибертехник умной среды, консультант по безопасности личного профиля, проектировщик интерфейсов беспилотной авиации, архитектор информационных систем, ИТ-проповедник, сетевой юрист, разработчик моделей больших данных, проектировщик промышленной робототехники, белый хакер, инженер по искусственному интеллекту... Слабым местом подготовки ИТ-специалистов (как и вообще подготовки специалистов

в высшей школе) является отрыв теоретических знаний от практики. Динамично развивающаяся область компьютерно-цифровых знаний нередко остается за рамками традиционной системы образования.

Существующая система подготовки ИТ-специалистов не справляется с возрастающими требованиями динамично развивающейся ИТ-индустрии. Разрыв между требованиями практики, реальной экономикой, и способностями и возможностями высшей школы увеличивается.

Цифровое поколение и особенно поколение Z (сетевое поколение) отличается своими личностными качествами от поколения индустриальной цивилизации. Для этого поколения характерны мобильность и гибкость мышления, клиповые знания и умение работать в условиях многозадачности, способность быстро воспринимать информацию и мгновенно переключаться с одного дела на другое. Это поколение испытывает субъективную зависимость от современных гаджетов, интернета и соцсетей, что приводит к трудностям в реальном социуме, в реальном общении и отсутствию присущих личности глубоких межличностных отношений. У этого поколения авторитетом являются не герои и родители, учителя и преподаватели, а всезнающий интернет. Отсюда почти абсолютная убежденность в своей правоте. Свои знания они черпают не из учебников и учебных занятий, не из классической художественной литературы, а собирают информацию из интернета, но не способны ее структурировать. Требуются иные подходы к системе обучения, которые обеспечат получение глубинных знаний, а интернет останется дополнительным источником информации.

Закключение. Общество в лице государства предоставило ИТ-специалистам и ИТ-бизнесу необходимые полномочия для создания самостоятельного независимого от иностранных ИТ-компаний собственного отечественного ИТ-бизнеса. Проводимый государством налоговый маневр (предоставление налоговых льгот) связан с расходами бюджета, включая налоговые послабления, что определяет размер предоставляемых льгот и потери бюджета (недополучение налоговых поступлений - выпадающие налоговые поступления/доходы), которые должны быть покрыты после достижения поставленной цели. Эти вынужденные расходы общества, являясь пробелом государственного механизма управления, накладывают определенные обязательства на российский ИТ-бизнес, его руководство и его специалистов, которые несут ответственность как перед государством, так и перед Отечеством, обществом, населением.

Получая сегодня государственную поддержку, они должны в будущем вернуть ее в форме создания эффективного конкурентоспособного отечественного ИТ-бизнеса и возросших налоговых поступлений в федеральный бюджет.

Введение налоговых преференций для ИТ-отрасли недостаточно, требуются инвестиции, дополнительное государственное и частное финансирование. Эта льготная налоговая программа даст желаемый эффект, если срок ее действия будет не менее 5 лет, по окончании установленного срока не должно быть резкого скачка ставок.

Следующий шаг должен привести к созданию отечественного внутреннего и внешнего рынка сбыта отечественного софта и электронной продукции, что требует дополнительных государственных мер по формированию платежеспособно-

го спроса со стороны отечественных организаций, включая компании МСП и население. Это значит расширить налоговые льготы и иные методы господдержки на всю область МСП как потребителей отечественного софта, а также обеспечить реальный рост доходов населения, которое представляет огромный рынок потребителей. Эта господдержка покупателей может выступить в прямой или модернизированной форме кэшбэк, как это сделано для туристического бизнеса. В любом случае крайне важна поддержка покупателей, которые стимулируют бизнес не только наращивать производство, но также совершенствовать продукцию. В итоге, повышается его конкурентоспособность. Стимулировать следует не только разработчика, но и потребителя отечественной продукции.

Для развития и поддержки МСП (помимо уже существующей финансовой поддержки) необходимо создать платежеспособный потребительский рынок, способный потреблять продукцию МСП, т.е. повысить доходы домашних хозяйств и заработную плату работающего населения. Можно увязать размер налога с величиной фонда заработной платы и размером заработной платы каждого работника: чем больше объем фонда заработной платы и размер заработной платы работника, тем меньше налоговое бремя и обязательные страховые взносы, т. е. ввести обратно пропорциональную зависимость.

Делая ставку на усиленно интенсивное развитие IT-отрасли, законодательная и исполнительная власть должны учитывать и другую сторону — социальную сферу, в том числе пенсионную систему, которая напрямую зависит от налогооблагаемой базы, размера ставки страховых отчислений и эффективности использования пенсионных накоплений. Крайне важно, решая проблемы пополнения пенсионного фонда и государственного бюджета, не метаться между повышением и снижением налоговых ставок, а постоянно и целенаправленно расширять налогооблагаемую базу путем увеличения количества налогоплательщиков — компаний МСП и эффективно рационального использования денежных средств пенсионного фонда с целью увеличения этих денежных ресурсов, относящихся к категории длинных денег.

Список литературы

1. IT-кадры: ступени образовательного роста. URL: https://akvobr.ru/it_kadry_stupeni_rosta.html (дата обращения: 17.06.2022).
2. IT-отрасль в России и в мире: как растет рынок информационных технологий. URL: <https://delprof.ru/press-center/open-analytics/it-otrasl-v-rossii-i-v-mire-kak-rastet-rynok-informatsionnykh-tehnologiy/> (дата обращения: 27.01.2022).
3. К вопросу подготовки кадров для IT-отрасли в условиях цифровизации. Юлия О. Климова; Владимир С. Усков. Вологодский научный центр РАН, Россия, г. Вологда. URL: <https://cyberleninka.ru/article/n/k-voprosu-podgotovki-kadrov-dlya-it-otrasli-v-usloviyah-tsifrovizatsii> (дата обращения: 15.06.2022).
4. Как будет восстанавливаться IT-рынок во втором полугодии 2022 года. URL: <https://trends.rbc.ru/trends/industry/62b45bf39a79471ff8e07d8e> (дата обращения: 28.07.2022).
5. Кириенко назвал число санкций, введенных против России. URL: <https://ria.ru/20220810/sanktsii-1808569740.html> (дата обращения: 10.08.2022).

6. Количество вводимых против России санкций продолжает расти. URL: <https://www.kommersant.ru/doc/5423114> (дата обращения: 21.06.2022).

7. Налоговые льготы для ИТ-компаний в России. URL: https://www.tadviser.ru/index.php/Статья:Налоговые_льготы_для_ИТ-компаний_в_России (дата обращения: 17.06.2022).

8. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_328854/ (дата обращения: 17.06.2022).

9. Письма Минфина России от 25.11.2021 № 03-15-09/95324, от 27.09.2021 № 03-15-06/78062, от 23.11.2020 N 03-03-06/1/101948 // СПС «КонсультантПлюс».

Д. А. Пискунов,

студент,

Российский университет дружбы народов

П. С. Лесникова,

студент,

Российский университет дружбы народов

КОНКУРЕНЦИЯ В СФЕРЕ 5G-ТЕХНОЛОГИЙ И МЕСТО РОССИИ

Аннотация. В настоящей статье исследуется актуальное состояние конкуренции между ведущими технологическими державами и место России в ней. Россия находится на этапе развития отечественных технологий и ставит разработку передового оборудования во главу угла. В рамках данной статьи ставится цель исследовать цепочку распространения технологий 5G в России и выделить факторы, которые действуют на развитие сетей нового поколения связи. Для достижения поставленной цели используется концепция трансфера технологий К. Краузе и реляционную модель представления данных. С помощью реляционной модели исследуются акторы, участвующие в процессе развития сетей 5G в России. В результате исследования приводятся факторы, влияющие на развитие 5G-технологий в России. Данная работа выполнена в рамках проекта «Технология анализа возможностей рынка 5G в зависимости от политических, экономических и социальных факторов (в развивающихся странах)».

Ключевые слова: США, КНР, 5G, технологическая конкуренция, Россия, Huawei, Ericsson, Nokia

5G-COMPETITION AND RUSSIA'S PLACE IN IT

Abstract. The present paper examines the current state of competition between leading technological powers and Russia's place in it. Russia is at the stage of domestic technology development and puts the development of advanced equipment at the top of its agenda. In the present article the authors aim to examine the chain of 5G technologies diffusion and single out factors that influence the development of 5G networks in Russia. To achieve this goal the authors, apply the concept of technology transfer described by

K. Krause and relational model for data representation. Using the relational model, the authors explore actors involved in the process of developing 5G networks in Russia. As a result of the study, the authors cite factors influencing the development of 5G technologies in Russia. The present article is completed as a part of the project «Technologies for analyzing the prospects of 5G markets depending on political, economic and social factors (in developing countries)».

Keyword: US, China, Russia, 5G, technology competition, Huawei, Ericsson, Nokia

Введение. Информационно-коммуникационные технологии стали влиять на социально-экономическое развитие государства. В этом контексте особое место занимает развитие инноваций (emerging technologies), в том числе технологий нового поколения связи (5G). Развитие 5G-сетей обусловлено увеличивающимся потреблением данных и растущим количеством телекоммуникационных устройств, что требует больших вычислительных мощностей и увеличение скорости обработки данных. Это также влияет на развитие сопутствующих передовых технологий, таких как облачные вычисления, Интернет вещей (IoT), искусственный интеллект и т. д.

Ведущие технологические государства, в том числе США, КНР, страны Западной Европы, уже запустили коммерческое использование сетей 5G, в то время как Россия и ряд развивающихся стран еще находятся на пути к полноценному развертыванию сетей нового поколения связи. Это связано с рядом сложностей, в первую очередь отсутствием регулирования в этой сфере, доступных радиочастот для тестирования и развертывания сетей нового поколения и экономическими издержками.

В рамках данной работы исследуется глобальная конъюнктура на рынке 5G-технологий и место России на этом рынке. Конфликт США и КНР в 2018 г. доказал значимость 5G-технологий с точки зрения экономического развития, национальной безопасности и глобального влияния. В результате этого США запретили технологическим компаниям КНР доступ на внутренний рынок, инвестирование в перспективные отрасли ИКТ и экспорт оборудования 5G. На данный момент Россия не создала собственного оборудования в сфере 5G-технологий, чтобы обеспечить функционирование критической инфраструктуры на основе отечественного оборудования. Однако над разработкой отечественных технологий работают ряд институтов и компаний, сотрудничающих с внешними компаниями.

Для анализа распространения 5G-технологий в России следует опираться на теорию трансфера технологий К. Краузе и использовать для представления данных реляционные модели. Теоретическая концепция позволяет анализировать диффузию технологий 5G и взаимоотношения между акторами в рамках системы трансфера технологий. Выстроить цепочку диффузии технологий и проанализировать факторы, влияющие на этот процесс.

Таким образом, данная статья исследует факторы развития 5G-сетей в России и место России в этой сфере. Раздел II выявляет роль и место данной

работы в исследовательском контексте. В разделе III объясняется концепция трансфера технологий и приводится общий вид реляционной модели, показывающей цепочку распространения технологий. Раздел IV – анализ политики основных акторов, США, КНР, ЕС, и механизмов распространения технологий 5G. Раздел V – актуальное состояние 5G сферы в России и выявляет институты, участвующие в развитии сетей 5G в России. В разделе VI выделяются сценарии развития сферы 5G в России и ключевые факторы, влияющие на развитие этой отрасли. В заключительном разделе приводятся результаты анализа и ключевые тенденции в сфере 5G в России.

Обзор литературы. Технологическая конкуренция в сфере 5G привлекла внимание как отечественных, так и зарубежных исследователей. Особую роль в исследовательском контексте играют базы данных по распространению 5G технологий, среди которых необходимо отметить «Карта технологических гигантов Китая» [21. С. 21–23], «Китайский Huawei выигрывает гонку 5G» [22] и «США vs КНР: контуры глобальной конкуренции» [23]. В рамках 1 проекта Австралийский институт стратегической политики исследует вопросы технологической безопасности, возникающие в результате использования 5G, и китайскую технологическую экспансию [21. С. 19–20]. Второй проект, реализуемый Советом по внешней политике [22], исследует тему с точки зрения политики США по ограничению Huawei как на внутреннем, так и на внешнем рынке. В конце концов, отечественный проект, проводимый кафедрой ТИМО РУДН, рассматривает конкуренцию США и КНР в отрасли 5G как аспект технологической зависимости страны от импорта оборудования и стандартов сети 5G.

Отечественные авторы отмечают, что ужесточенная политика США в отрасли 5G-технологий главным образом связана с возможностью Huawei занять позиции лидера в разработке и производстве оборудования для нового поколения связи [4. С. 111; 6. С. 22; 7. С. 40]. Ряд зарубежных авторов придерживается позиции, согласно которой использование 5G-технологий влечет вызовы и угрозы национальной безопасности [20. С. 54; 21. С. 20; 24. С. 92]. Определенный пласт работ рассматривает конкуренцию в сфере передовых технологий (5G) как транзит власти в технологической сфере от США к КНР и смену глобального мирового порядка [14. С. 242, 32. С. 37, 34. С. 77]. Касательно проблематики создания 5G-сетей в России отечественные авторы анализируют проблемы и факторы развития технологий пятого поколения связи, обращая внимания на законодательные, политические и экономические барьеры [10. С. 117–119; 18. С. 458].

Методология. В качестве методологической основы используется теоретическая концепция трансфера технологий К. Краузе. Согласно К. Краузе, трансфер технологий представляет иерархическую систему, в рамках которой государства, владеющие передовыми разработками, занимают высшее положение и управляют трансфером технологий в целях не допустить оттока критических для национальной безопасности технологий и сохранить влияние на международной арене [26. С. 701]. Так, например, растущая мощь Японии во второй половине XX в. заставила США ужесточить экспортный контроль и ограничить трансфер чувствительных технологий [8. С. 95]. На низшей ступени иерархической системы нахо-

дятся государства, зависимые от импорта технологий. Между ними расположены еще 2 ступени, которые занимают акторы с более и менее развитым технологическим сектором [9. С. 44]. В контексте современной структуры производства в сфере ИКТ авторы понимают, что теория не учитывает такие факторы, как глобализация, международное разделение труда и т. д. Однако теория подчеркивает, что государства в сфере 5G-технологий конкурируют за положение ведущего актора в иерархии трансфера технологий, а страны-импортеры, в свою очередь, выступают как объект такой конкуренции.

Рассматривая 5G-сети в качестве критического элемента национальной безопасности, можно сказать, что разработка собственных технологий указывает на положение государства в рамках иерархии К. Краузе. Так, США, КНР и ЕС занимают ведущее положение, так как располагают своими технологиями [5. С. 169]. Россия, в свою очередь, только инвестирует в развитие технологий 5G и вырабатывает стандарты и регулирования в данной сфере.

Используя методику построения реляционных моделей, исследуется цепочка распространения 5G-технологий, в рамках которой выделяется 4 субъекта («сущности»): страна, поставщик инфраструктуры, мобильный оператор и головная организация (материнская компания/государственная организация). Все 4 субъекта взаимосвязаны между собой и участвуют в процессе распространения 5G-технологий. Страна выступает как место создания тестирования 5G-технологий и определяет внутреннее регулирование, занимается распределением радиочастот и проводит аукционы по развитию 5G-сетей. Поставщик инфраструктуры представлен телекоммуникационной компанией, которая предоставляет свое оборудование для развертывания сети. Мобильный оператор занимается предоставлением услуг связи в конкретной стране и использует установленное оборудование 5G для тестирования или коммерческого использования. Головная организация может быть представлена холдингом (группой компаний) или государственной организацией, которая контактирует с поставщиками оборудования и занимается вопросами поставки (рис. 1).

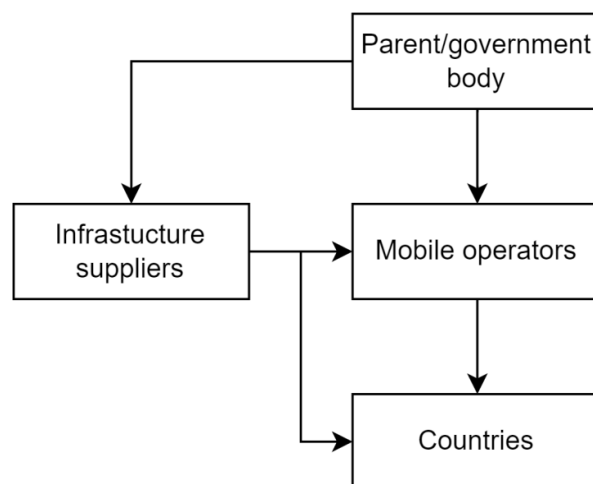


Рис. 1. Реляционная модель распространения 5G-технологий

Основные акторы в сфере 5G и механизмы конкуренции. Ввиду стремительного увеличения объема производимых данных, возросшей роли ИКТ для экономического развития государств передовые технологии играют большую роль на иностранных рынках. Одним из аспектов конкуренции ведущих технологических стран является соперничество за распространение технологий 5G, так как лидерство в этой сфере обеспечит ряд преимуществ государству и технологическим компаниям.

Во-первых, компания получает доступ к национальной инфраструктуре и производимым в стране данным, которые являются двигателем развития технологий. Во-вторых, первенство в рамках нового поколения связи (5G) позволит развивать новые стандарты связи и протоколы (New IP), которые будут отвечать интересам компаний и стран лидеров [33. С. 20]. В-третьих, так как технологии являются драйвером развития, распространение технологий становится инструментов политического давления или рычага силы для того или иного государства. США, КНР, Корея и страны Европы представляют своих поставщиков оборудования, конкурируя за иностранные рынки. Рынок стран ЮВА является одним из наиболее перспективных для распространения передовых технологий. На данный момент можно выделить 5 основных поставщиков оборудования – Huawei, ZTE (оба КНР) [19], Ericsson (Швеция), Nokia (Финляндия), Samsung (Корея).

Для того чтобы ограничить распространение китайских технологий, США и ЕС используют ряд механизмов. В первую очередь Соединенные Штаты выдвинули инициативу «Чистая сеть» («Clean network») в 2020 г. Целью инициативы стало создание глобального альянса, в рамках которого используется оборудования от «надежных» поставщиков. Иными словами, программа была направлена на ограничение китайских компаний (Huawei, ZTE) в мире. В 2022 г. страны 4-стороннего диалога по безопасности (QUAD) приняли Меморандум о сотрудничестве по диверсификации поставщиков 5G и Open RAN [28] и создали Open RAN Policy Coalition [29]. Оба механизма направлены на повышение совместимости технологий, безопасности их использования и увеличение количества поставщиков оборудования.

Европейский союз принял Инструментарий по безопасности 5G (EU Toolbox for 5G security), в котором выделены 5 сценариев с высоким риском развития 5G технологий [31]. В программе «Чистая сеть» принимают участие не только государства, но и телекоммуникационные компании, которые осуществляют свое присутствие в других регионах с помощью мобильных компаний (дочерних предприятий). К таким компаниям можно отнести Telefonica (Испания), Orange (Франция), Jio (Индия), Telstra (Австралия), SK Telecom (Корея), O2 (Великобритания), AT&T (США) и др. [30]. Таким образом, это свидетельствует о том, что телекоммуникационные компании также участвуют в процессе распространения 5G-технологий.

Китай, в свою очередь, продвигает технологии в сфере телекоммуникации посредством как глобальных проектов, так и региональных. Главным из них является инициатива «Пояса и пути» (Belt and Road initiative), в рамках которой в 2018 г. кристаллизовалась программа «Цифрового шелкового пути» (Digital Silk Road) [20. С. 53]. Именно благодаря этим проектам, как отмечают исследователи

Австралийского института стратегической политики (Australian Strategic Policy Institute), Китай осуществляет технологическую «экспансию» в развивающихся странах, устанавливая технологии искусственного интеллекта, системы общественной безопасности «Умный город» и т. д. В рамках стратегии Информатизации Китай поставил цель создать международную мобильную сеть с использованием отечественных технологий к 2025 г.

Таким образом, можно сделать вывод, что отрасль 5G представляет особую область конкуренции для ведущих государств, так как лидерство в сфере ИКТ приносит ряд выгод как государству, так и ИКТ-компаниям.

Актуальное состояние 5G-отрасли в России. На данный момент в России нет повсеместно распространенных 5G-сетей, при этом в таких крупных городах, как Москва, Санкт-Петербург, Нижний Новгород, Иннополис и так далее саму технологию тестируют, т. е. сейчас 5G-отрасль в РФ находится на подготовительном этапе. Пилотные зоны для тестирования технологии имеются у МТС, «Теле-2», «Мегафон» и «Билайн» [2. С. 271]. Лицензия на оказание 5G-услуг есть только у МТС.

Одной из ключевых проблем по запуску коммерческого 5G в России стал недопуск к нужным частотам (3,4–3,8 ГГц), необходимых для 5G, так как эти частоты используются для нужд Минобороны и Роскосмоса, поэтому операторам приходится искать альтернативы. В 2019 г. президент Путин согласился с письмом Совета безопасности РФ, в котором говорилось о недопустимости использования частот 3,4–3,8 ГГц для сетей 5G. Ранее в том же году Министерство обороны РФ опубликовало отрицательный отзыв о предложенной Концепции развития технологий 5G в России, подготовленной Министерством связи, и отказалось предоставить необходимые частоты.

В 2022 г. НИИ Радио вместе с Huawei начали тестировать в Москве оборудование для 5G в диапазоне 6,4–7,1 ГГц [13]. Приоритетным диапазоном для развертывания 5G является 4,8–4,99 ГГц, какой, например, используется в Китае и Японии. Экосистема оборудования с поддержкой данного диапазона хуже развита. Далеко не все модели пользовательских устройств (смартфонов и пр.) и базовых станций смогут работать в российских 5G-сетях. Операторам и абонентам придется выбирать из меньшего количества моделей. Более того, обеспечить масштабное покрытие в этом диапазоне будет слишком дорого, он больше подходит для охвата центральных районов городов с наибольшей плотностью жителей.

Что касается оборудования для предоставления услуг 5G, то важно отметить, что на данный момент отсутствует серийное отечественное оборудование. Это означает, что РФ вынуждена использовать оборудование иностранных поставщиков. Это в первую очередь Huawei, а также ZTE. Это можно объяснить тем, что в 2019 г., когда для тестирования 5G выделили диапазон 4,8–4,99 ГГц, его поддерживали только базовые станции китайской компании [25].

Ряд экономических и политических факторов ставит китайские компании Huawei и ZTE в сильное положение, но, несмотря на тесные партнерские отношения между Москвой и Пекином, российские власти не собираются предоставлять китайским телекоммуникационным гигантам эксклюзивные преференции. В отличие от ряда западных государств, которые видят в Huawei угрозу национальной

безопасности и ограничивают распространение китайских технологий [16], российскими мобильными операторами движут в основном коммерческие интересы. Если Москва не сможет обойтись без иностранного участия в разработке технологий 5G, она попытается диверсифицировать свое сотрудничество с зарубежными поставщиками.

В целях диверсификации помимо Huawei российские компании используют оборудование и других вендоров, таких как Ericsson и Nokia.

Российский телекоммуникационный рынок привлекателен для иностранных вендоров. По данным NeoAnalytics, в 2020 г. он вырос на 21 % и составил 1,15 трлн рублей (15,7 млрд долл.) [25]. Учитывая размеры страны и отсутствие покрытия сетей LTE на отдаленных территориях России, российский рынок остается чрезвычайно перспективным.

Если коснуться общих тенденций в использовании иностранного оборудования с целью предоставления мобильной связи, то важно отметить, что мобильные операторы официально не раскрывают долю своей инфраструктуры, приходящуюся на отдельных вендоров. Однако данные о закупках, публикуемые операторами, а также информация об аутсорсинговых соглашениях дают основания сделать следующие выводы.

Согласно имеющимся данным, в Центральном федеральном округе сети «Билайн» работали преимущественно на технологиях европейских вендоров, а в Северо-Западном федеральном округе – на оборудовании Huawei. «МегаФон» в основном работал с Nokia в Центральном федеральном округе (ЦФО), включая Москву и Московскую область, и в Северо-Кавказском федеральном округе (СКФО), а Huawei контролирует сети в Северо-Западном (СЗФО) и Приволжском федеральных округах (ПФО), Сибири и на Дальнем Востоке (ДФО). В некоторых регионах (Челябинск, Оренбург, Чувашия) технологию предоставляет другой китайский вендор ZTE. Операторы МТС и Tele2 в основном работали с Ericsson. Ее технологии поддерживали МТС в Сибирском, Уральском и Южном федеральных округах. Nokia отвечало за сети прошлого поколения в Северо-Западном округе, а высокоскоростные сети LTE работают на технологии Samsung. Tele2 минимально использовал оборудование Huawei, предпочитая европейских вендоров Ericsson и Nokia.

Четыре ведущих мобильных оператора связи в России используют различных поставщиков оборудования, чаще всего выбирая Huawei, Ericsson и Nokia (рис. 2). Стоит отметить, что среди перечисленных провайдеров только Veon Ltd. является зарубежным телекоммуникационным холдингом, который зарегистрирован в Нидерландах. Дочерняя компания Veon Ltd., «Билайн» тестирует сети 5G, используя как технологии европейских, так и китайских поставщиков. Исходя из рис. 2, можно сказать, что российские мобильные операторы развивают сотрудничество как с европейскими, так и с китайскими поставщиками, руководствуясь экономической выгодой в развитии сетей 5G.

В этой связи стоит отметить, что выбор поставщиков может зависеть от ряда факторов, в том числе политический и технологический. Политический фактор указывает на то, что сотрудничество России и Китая в политической сфере предполагает трансфер технологий, в том числе в сфере 5G. Помимо этого, полити-

ческий фактор стал играть более значимую роль после того, как Ericsson и Nokia отказались от поставок в Россию в феврале – марте 2022 г. [27]. Это, с одной стороны, усложняет попытки диверсификации поставщиков, но, с другой стороны, является возможностью для развития собственных технологий. В свою очередь, технологический фактор оказывает следующее влияние.

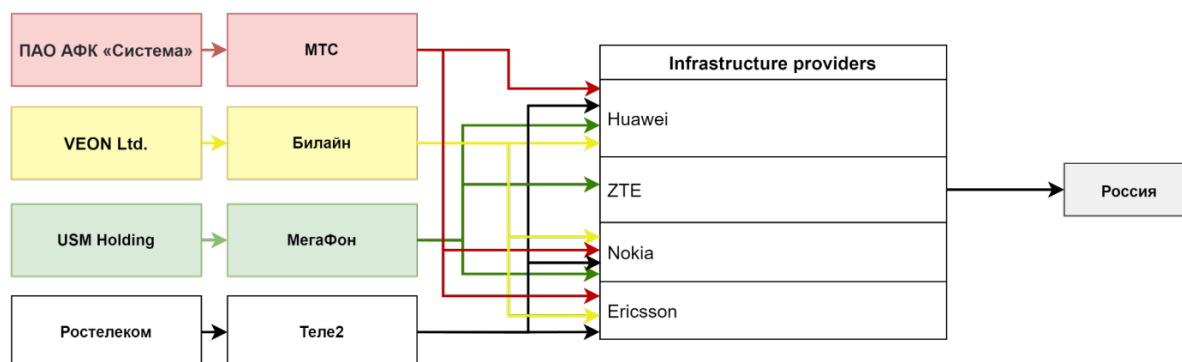


Рис. 2. Реляционная модель распространения технологий 5G в России

Ввиду того, что самый востребованный диапазон частот 3,4–3,8 ГГц недоступен для коммерческого использования, российские провайдеры выбирают технологии тех поставщиков, которые смогут работать в более высоких диапазонах, например, 4,8–4,99 ГГц.

Тем не менее российские инновационные компании, технологические центры стремятся к развитию собственного 5G-оборудования. К примеру, в 2021 г. МТС совместно с фондом «Сколково» и Сколтехом разработали программное обеспечение на основе открытой стандартизированной архитектуры радиодоступа Open RAN с использованием оборудования иностранных поставщиков [12]. Разработка ПО является важным шагом на пути к разработке собственного оборудования.

Государственная корпорация «Ростех» планирует начать выпуск базовых станций в 2024 г. [11]. Осенью 2019 г. его генеральный директор Сергей Чемезов заявил, что госкорпорация способна производить собственные технологии 5G и что первая экспериментальная сеть 5G на российском оборудовании может быть запущена в 2022–2023 гг. Чемезов также сказал, что возможна локализация производства, так что некоторые ключевые компоненты будут производиться только в России. Важно, чтобы технологии 5G производились внутри страны, уточнил он, поскольку, учитывая их потенциальное использование, они могут считаться критически важной инфраструктурой национальной безопасности. Полноценный запуск технологий 5G планируется к 2024 г. По уровню развития 5G Россия отстает от мировых лидеров на 3–5 лет.

Факторы и сценарии развития 5G-сетей в России. Научно-исследовательский институт связи в 2019 г. подготовил доклад, в котором обозначены 3 сценария развития 5G-сетей в России в зависимости от участия компаний в строительстве оборудования. В рамках первого сценария предполагается, что инфраструктура

будет строиться каждым оператором отдельно, что предполагает более высокие капитальные и операционные затраты. Второй вариант предполагает совместное строительство с помощью создания совместного предприятия (СП). Данный сценарий более выгодный и предлагает возможность равного участия всех операторов в создании инфраструктуры. В рамках третьего сценария вся инфраструктура будет создаваться одной организацией и впоследствии будет принадлежать только ей. Последний вариант предполагает наименьшие издержки для бизнес-сообщества, однако вся инфраструктура будет принадлежать одной организации [1].

В 2020 г. Федеральная антимонопольная служба (далее – ФАС) дала положительный ответ на ходатайство «Ростелеком», «МегаФон», «Вымпелком» и МТС о создании СП для развития 5G-сетей в России с условием равного использования инфраструктуры и доступа к радиочастотам 5G [3]. В 2021 г. ФАС одобрила просьбу «Ростелеком», «Башинформсвязь», «ВымпелКом» («Билайн») и «МегаФон» на создание СП [17]. По мнению информационных и консалтинговых агентств, ведущие операторы связи пытаются получить доступ к развитию 5G-сетей в диапазоне 3,4–3,8 ГГц, которые на данный момент принадлежат Министерству обороны РФ и Роскосмосу.

Сфера 5G-технологий может развиваться под действием ряда геополитических и экономических факторов.

В первую очередь необходимо отметить технологическую безопасность, в основе которой лежит политика России по развитию отечественных технологических отраслей. В этой связи технологии 5G позволят создать ядро сетей нового поколения связи на основе отечественных технологий, в том числе в диапазонах, используемых Министерством обороны РФ и Роскосмосом, и развивать дальнейшие сопутствующие технологии 6-го поколения.

Во-вторых, фактором развития нового поколения связи может стать реализации концепции «Умный город» в целом и распространение беспилотных автомобилей в частности. Для их функционирования требуется высокая производительность сети и низкая задержка в передачи данных. Работа беспилотных автомобилей не может быть обеспечена за счет нынешнего поколения связи.

В-третьих, ключевым фактором развития данной сферы могут стать Роскосмос и Министерство обороны РФ, в ведении которых находится диапазон 3,4–3,8 ГГц. Бывший глава государственной корпорации по космической деятельности «Роскосмос» Д. Рогозин отметил, что в рамках программы «Сфера» корпорация будет использовать спутники нового поколения связи [15]. Такая спутниковая связь сделает доступным широкополосную связь и Интернет вдоль всего Северного морского пути.

В свою очередь, применение 5G-технологий создаст возможности для использования роботов, беспилотной техники в военной сфере [10. С. 251].

Правовой аспект развития 5G-технологий. Технологии пятого поколения связи находятся в самом начале развития и открывают новые возможности для развития цифровой экономики и передовых технологий, в том числе Интернета вещей (IoT) и др. В этой связи мобильные провайдеры стали предлагать различные варианты обработки трафика, передаваемого через сети 5G, в зависимости от получателя услуги и потребностей используемого устройства. В 2015 г. пар-

ламент ЕС принял закон об открытом Интернете или Net Neutrality (NN). Орган европейских регуляторов электронных коммуникаций (BEREC) выпустил соответствующий руководящий документ в 2016 г., согласно которому поставщик услуг доступа в Интернет (IAS) должен одинаково относиться ко всему трафику, без дискриминации, ограничений или вмешательства, независимо от отправителя, получателя, контента, услуги, приложения или используемого устройства. Закон устанавливает требование быть нейтральным по отношению к обрабатываемым данным и получателя услуги. Бизнес-сообщество негативно отреагировало на данный закон, выпустив «Манифест по своевременному развертыванию 5G в Европе». Руководители BT, Deutsche Telekom, SK Hutchison, Orange, Proximus, KPN, Tele2, Telecom Italia, Telefonica, Telekom Austria, Telenor, Telia и Vodafone; производители инфраструктуры Ericsson, Nokia и спутниковые компании Inmarsat и SES предупредили об «опасности ограничительных правил сетевой нейтральности в контексте технологий 5G, бизнес-приложений и не только».

Соединенные Штаты Америки, озабоченные развитием 5G-сетей с точки зрения национальной безопасности, на национальном уровне одобрили закон Secure 5G and Beyond Act of 2020. Закон направлен на обеспечение национальной безопасности в сетях пятого поколения связи и выше. Ключевыми мерами по решению данной проблемы выбраны разработка стратегии безопасности в данной отрасли, оценка потенциала замещения оборудованием китайских на основе отечественных поставщиков и других поставщиков в странах, являющихся союзниками или стратегическими партнерами, а также определение стимулов и вариантов политики поддержки внутреннего производства оборудования и подготовки кадров. Россия находится только на этапе не только развития данной технологии, но и создания правовых подходов регулирования, поэтому, как было отмечено ранее, данная сфера развивается в рамках программы «Цифровая экономика РФ».

Выводы. Таким образом, сфера 5G-технологий представляет значимый потенциал для экономического развития и роста политического влияния государства. С точки зрения системы международных отношений лидерство в технологической сфере может поменять расстановку сил. В данном контексте ключевые акторы, такие как США, Китай, ЕС, конкурируют на рынке 5G и экспортируют свои разработки на развивающиеся рынки. Так как сфера технологий напрямую затрагивает вопросы национальной безопасности, государства выпустили ряд программ и предприняли политику продвижения своих компаний и ограничения других. В контексте такой конкуренции объектом становятся страны, которые импортируют технологии или только их развивают. К числу последних относится Россия, которая активно инвестирует в создание отечественных технологий 5G.

Анализируя распространение технологий 5G в России, можно сделать следующие выводы. Российские технические институты, инвестиционные фонды, технологические компании вовлечены в разработку отечественных технологий нового поколения связи. На данный момент уже разработано программное оборудование для оборудования 5G, созданного на открытой архитектуре Open RAN. Более того, в 2023 г. государственная корпорация «Ростех» планирует закончить разработку отечественного оборудования нового поколения связи. Вместе с тем

мобильные операторы тестируют и запускают сети 5G. Развитие указанных технологий до последнего момента шло под действием ряда факторов. Ключевым фактором стала недоступность радиочастот для тестирования сетей 5 поколения связи. Ввиду этого российские телекоммуникационные компании вынуждены выбирать другие диапазоны радиочастот, оценивать капитальные и операционные затраты и осуществлять поиск подходящего оборудования. Касательно политики использования технологий 5G, необходимо отметить, что в России использовались разработки как китайских, так и европейских поставщиков. Тем не менее в 2022 г. в связи с международными санкциями против России компании Ericsson и Nokia прекратили поставки оборудования в Россию. Это создает возможности для развития отечественных технологий и присутствия иностранных компаний.

Список литературы

1. 5G в России. – 2019. – April. – URL: https://www.cnews.ru/news/top/2019-04-03_5g_v_rossii_skolko_nuzhno_denegkogda_okupitsya (дата обращения: 29.08.2022).
2. Андрианов В. Д. Сотовая связь пятого поколения (G 5): мировые тренды и проблемы внедрения в России // Россия: тенденции и перспективы развития. – 2021. – № 16-2. – С. 268-275.
3. В России операторам разрешили объединиться для запуска сетей 5G. – 2021. – May. – URL: <https://www.ixbt.com/news/2021/05/04/v-rossii-operatoram-razreshili-obedinitjsja-dlja-zapuska-setej-5g.html> (дата обращения: 29.08.2022).
4. Гамза Л. А. Технологическое противостояние США и Китая в АТР // Россия и АТР. – 2020. – № . 3 (109). – С. 110-133.
5. Данилин И. В. Американо-китайская технологическая война: риски и возможности для КНР и глобального технологического сектора // Сравнительная политика. – 2020. – № 11 (4). – С. 160-176. DOI: 10.24411/2221-3279-2020-10056
6. Дегтерев Д. А., Рамич М. С., Пискунов Д. А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций. 2021. – Т. 16. – № 3. – С. 7-33.
7. Ефременко Д. В. Формирование цифрового общества и геополитическая конкуренция // Контуры глобальных трансформаций: политика, экономика, право. – 2020. – Т. 13. – № . 2. – С. 25-43.
8. Кириченко Э. Контроль США над международными каналами трансферта технологий: вызовы, механизмы, тенденции // Мировая экономика и международные отношения. – 2021. – Т. 65, № 7. – С. 89-97. DOI: 10.20542/0131-2227-2021-65-7-89-97
9. Мальцев А. Сетевая динамика «диффузии технологий» в системе международных трансфертов вооружений // Международные процессы. – 2020. – Т. 18, № . 4. – С. 36-61.
10. Манушин Д. В. Проблемы, перспективы и антикризисные меры в области развития технологии 5G // Вектор развития управленческих подходов в цифровой экономике: Материалы III Всероссийской научно-практической конференции, Казань. Казань: Издательство «Познание». – 2021. – С. 251.
11. Минцифры предоставит «Ростеху» около 21,5 млрд рублей на развитие 5G. – 2021. – June. – URL: <https://www.vedomosti.ru/technology/news/2021/06/30/876243-mintsifri-predostavit-rostehu-215-mlrd> (дата обращения: 29.08.2022).

12. МТС испытала 5G-оборудование Open RAN на отечественном ПО. – 2021. – November. – URL: <https://moskva.mts.ru/about/media-centr/soobshheniya-kompanii/novosti-mts-v-rossii-i-mire/2021-11-09/mts-ispytala-5g-oborudovanie-open-ran-na-otechestvennom-po> (дата обращения: 29.08.2022).
13. НИИ Радио исследует использование макетов оборудования 5G на базовой станции Huawei. // ТАСС. – 2021. – December. – URL: <https://tass.ru/ekonomika/13077161> (дата обращения: 29.08.2022).
14. Рамич М. С., Пискунов Д. А. Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов // Вестник Российского университета дружбы народов. Серия: Международные отношения. – 2022. – Т. 22. – № 2. – С. 238–255. DOI: 10.22363/2313-0660-2022-22-2-238-255
15. Россия с 2021 года начнет развертывание спутниковой группировки «Сфера» // ТАСС. – 2020. – October. – URL: <https://tass.ru/kosmos/9836399> (дата обращения: 01.08.2022).
16. США официально признали Huawei и ZTE угрозой национальной безопасности. – 2020. – June. – URL: <https://www.interfax.ru/world/715397> (дата обращения: 29.08.2022).
17. ФАС одобрила операторам связи заключение соглашения по построению сетей стандарта 5G. – 2021. – May. – URL: <https://fas.gov.ru/news/31275> (дата обращения: 29.08.2022).
18. Фомина А. Н. Развитие инновационных технологий 5G в телеиндустрии: проблемы и перспективы // Вопрос инновационной экономики. – 2022. – Т. 12. – № 1. – С. 449–462.
19. Australian strategic policy institute. URL: <https://chinatechmap.aspi.org.au/#/homepage> (дата обращения: 2.09.2022).
20. Bartholomew C. China and 5G // Issues in Science and Technology. – 2020. – 36 (2). – Pp. 50–57.
21. Cave D. Mapping China's Technology Giants // Australian Strategic Policy Institute. – 2019. – № 15. – 25 p.
22. Council on Foreign Relations. – 2021. – March. – URL: <https://www.cfr.org/blog/china-huawei-5g> (дата обращения: 2.09.2022).
23. G2 Research Project. URL: <https://g2.rudn.ru/page/about-research> (дата обращения: 2.09.2022).
24. Harold S. W., Kamijima-Tsunoda R. Winning the 5G race with China: a US-Japan strategy to trip the competition, run faster, and put the fix in // Asia policy. – 2021. – Т. 28. – № 3. – С. 75–103.
25. Kovachich L. Who will get a slice of Russia's 5G pie? – 2021. – December. – URL: <https://carnegiemoscow.org/commentary/86092> (дата обращения: 29.08.2022).
26. Krause K. (1990). The Political Economy of the International Arms Transfer System: The Diffusion of Military Technique via Arms Transfers // International Journal. – 1990. – vol. 45. – № 3. – Pp. 687–722. DOI: 10.2307/40202695
27. Nokia заставили отказаться от поставок в Россию. – 2022. – March. – URL: https://www.cnews.ru/news/top/2022-03-02_nokia_zastavili_otkazatsya (дата обращения: 29.08.2022).

28. OpenRAN Policy Coalition. – 2022. – May. – URL: <https://www.openranpolicy.org/statement-on-the-quad-leaders-tokyo-summit-2022/> (дата обращения: 2.09.2022).

29. Quad Joint Leaders' Statement. – 2022. – May. – URL: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/> (дата обращения: 01.08.2022).

30. The Clean network. URL: <https://2017-2021.state.gov/the-clean-network/index.html> (дата обращения: 01.08.2022).

31. The EU toolbox for 5G security. – 2021. – March. – URL: <https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security> (дата обращения: 01.08.2022).

32. Toledo D. G.C., Toledo J. E.C. Technological transition and technological dependency: Latin America – China relations in a changing international order // Revista de Gest?o. – 2021. Pp. 35–44.

33. Tugendhat H., Voo J. (2021). China's Digital Silk Road in Africa and the Future of Internet Governance // Working Papers – 2021. – № 50. – 26 p.

34. Wong, P. N. Techno-Geopolitics: US-China Tech War and the Practice of Digital Statecraft // Routledge India. – 2021. – 134 p.

А. А. Прибытко,

аспирант юридического факультета,

Белорусский государственный университет

ПРАКТИКА ИНВЕСТИЦИЙ В РЕСПУБЛИКЕ БЕЛАРУСЬ В РАМКАХ ПАРКА ВЫСОКИХ ТЕХНОЛОГИЙ

Аннотация. Привлечение инвестиций и развитие высокотехнологического производства являются важными факторами роста экономики. В данной статье рассматривается практика Республики Беларусь по созданию специального правового режима регулирования деятельности по разработке высокотехнологичных продуктов, введенного в целях привлечения инвестиций в страну. Научная новизна заключается в исследовании вопроса взаимосвязи специального правового режима и инвестиционной привлекательности региона.

Ключевые слова: право, цифровые технологии, инвестиции, IT-отрасль, регион, инфраструктура, инновации

THE PRACTICE OF INVESTMENTS IN THE REPUBLIC OF BELARUS ON THE EXAMPLE OF A HIGH-TECH PARK

Abstract. Attraction of investments and development of high-tech production are among the most important factors of economic growth. This article discusses the practice of the Republic of Belarus on the creation of a special legal regime for regulation of the development of high-tech products, introduced in order to attract investment to the country. Scientific novelty is in the research of the relationship between the special legal regime and the investment attractiveness of the region.

Keywords: Law, Digital technologies, Investments, IT industry, Region, Infrastructure, Innovation

На современном этапе важным фактором повышения инвестиционной привлекательности государства и, соответственно, привлечения инвестиций является уровень развития высоких технологий, который зачастую обусловлен уровнем поддержки данной отрасли экономики со стороны государства. Сфера высоких технологий, без преувеличения, считается драйвером экономик, имеющим безграничный потенциал для роста.

Республика Беларусь заслужено имеет статус страны, славящейся своей школой информационных технологий. Нормативную правовую основу регулирования сферы высоких технологий в Республике Беларусь составляет Положение о Парке высоких технологий, утвержденное Декретом Президента Республики Беларусь от 22.09.2005 № 12 (в ред. декрета Президента Республики Беларусь от 21.12.2017 № 8) (далее – Положение) [1, 2].

Парк высоких технологий (далее – ПВТ) – это специальная экономическая зона-статус, позволяющая резидентам ПВТ, зарегистрированным в качестве таковых и осуществляющим деятельность в сфере информационных технологий, получить предусмотренные законодательством льготы и преференции.

ПВТ основан в 2005 г. и изначально рассматривался в качестве потенциальной основы повышения конкурентоспособности экономики Беларуси в сфере высоких технологий. Позже идеи трансформировались в создание на основе парка базы инновационных производств, основанных на высоких технологиях, консолидации кадрового и технологического базиса для дальнейшего перехода экономики к цифровому уровню.

Основными направлениями деятельности ПВТ являются:

- разработка и экспорт информационно-коммуникативных технологий;
- привлечение инвестиций в сферу высоких технологий со стороны отечественных и зарубежных источников;
- внедрение новых технологий в уже существующие сферы экономики с целью увеличения производительности труда.

Управлением деятельности ПВТ занимается Администрация, которая является государственным учреждением. Наблюдательный совет Администрации осуществляет общую координацию деятельности ПВТ, в том числе проверку требований к содержанию предлагаемых ими бизнес-проектов, регистрацию юридических лиц и (или) индивидуальных предпринимателей в качестве резидентов ПВТ, а также контролирует порядок осуществления ими деятельности в качестве резидентов ПВТ.

В ПВТ зарегистрировано около 1065 резидентов и более 78 тысяч работников. Экспорт резидентов ПВТ в 2021 г. составил \$ 3,2 млрд при темпе роста 118,9 %, что составляет примерно 30 % всего экспорта услуг Беларуси. Внешнеторговое сальдо ПВТ в 2021 г. составило \$ 2,8 млрд [3].

Успешный опыт ПВТ также используется в других сферах и направлениях. Так, были созданы аналоги ПВТ:

1) Китайско-белорусский индустриальный парк «Великий камень» – для разработки совместных проектов, интеграции и промышленной унификации с китайской стороной, привлечения инвестиций и технологий;

2) Национальный научно-технологический парк «БелБиоГрад», основной профиль которого научные исследования и создание инвестиционных проектов в сфере высокотехнологичных производств.

Наиболее важным аспектом ПВТ является то, что он построен по экстерриториальному принципу. Это означает возможность использования преимуществ правового режима ПВТ любому лицу, отвечающему установленным требованиям, безотносительно места его регистрации на территории Республики Беларусь. Иными словами, речь идет об определенном юридическом статусе субъекта, зарегистрированного в качестве резидента ПВТ, что позволяет ускорить процесс интеграции и обмена знаниями или опытом.

В качестве резидентов ПВТ могут быть зарегистрированы юридические лица и индивидуальные предприниматели Республики Беларусь, осуществляющие или планирующие осуществлять виды деятельности, связанные с разработкой информационных технологий, по перечню, предусмотренному законодательством.

Отдельные виды деятельности разрешено осуществлять только будучи зарегистрированным в качестве резидента ПВТ. Такой подход представляется верным, так как многие современные технологии и экспериментальные виды деятельности сопряжены с мошенничеством и риском причинения вреда общественным интересам. К таким видам деятельности относятся, например, облачные вычисления, блокчейн технологии, криптовалюты и токены [4].

Помимо существующих административных и процессуальных процедур, обязательным условием для регистрации в качестве резидента ПВТ является предоставление бизнес-плана по осуществлению деятельности, связанной с разработкой и реализацией информационных проектов. В бизнес-плане указывается профиль и виды деятельности субъекта, инвестиционный план, вид готового товара или услуги, способ получения прибыли (монетизации) и необходимость в данном виде продукции. Также возможно указать и представить продукт компании, находящийся на стадии прототипа или опытный образец технологии.

Отметим, что резиденты ПВТ не вправе получать выручку (доход) от осуществления видов деятельности, отличных от заявленных ими при регистрации в качестве резидента ПВТ или прямо не разрешенных соответствующими законодательными актами. При необходимости изменения существующей стратегии предприятия, резидент ПВТ имеет право заниматься иными видами, не согласованными в первом бизнес-плане, только после внесения изменений в бизнес-план и прохождения повторной процедуры его одобрения Наблюдательным советом Администрации ПВТ.

Основой стимулирования роста и привлечения инвестиций можно послужила налоговая политика, реализуемая государством в отношении резидентов ПВТ.

Резиденты ПВТ обязаны перечислять 1 % от выручки в пользу Администрации ПВТ. Вместе с тем при соблюдении обозначенных законодательством условий резиденты ПВТ имеют право на следующие основные льготы:

- 1) освобождение от налога на прибыль (в отдельных случаях – пониженная ставка налога на прибыль);
- 2) освобождение от уплаты НДС;
- 3) освобождение от уплаты оффшорного сбора (за рекламные, маркетинговые, посреднические услуги; выплачиваемые дивиденды);
- 4) освобождение от налога на недвижимость (в отношении объектов, расположенных на территории ПВТ (за исключением, сдаваемых ими в аренду);

5) освобождение от земельного налога.

Также предусмотрены льготы для иностранных участников резидентов ПВТ и нерезидентов, оказывающих услуги резиденту ПВТ. Например, пониженные и нулевая ставки по налогу на доходы иностранных организаций, не осуществляющих деятельности в Республике Беларусь через постоянное представительство (налогообложение у источника).

Такая модель построения налоговых обязательств свидетельствует о том, что направленностью ПВТ является не столько сбережение, сколько повышение оборотоспособности денежных средств у резидентов ПВТ и их постоянная реинвестиция.

Законодательством также определен ряд иных преимуществ, льгот, преференций, особых условий и порядка осуществления предпринимательской деятельности компаний резидентов ПВТ. Так, например:

- первичные учетные документы могут формироваться и приниматься в более упрощенном порядке, в отличие от установленной строгой формы бухгалтерской отчетности;

- часть доходов, получаемых работниками ПВТ в рамках профессиональной деятельности у резидентов ПВТ, не облагаются взносами на социальное страхование;

- право применения льготного коэффициента на аренду помещений;

- возможность привлекать граждан других государств или лиц без гражданства для работы в рамках организаций резидентов ПВТ по упрощенному порядку.

Также только резиденты ПВТ вправе применять в рамках осуществления хозяйственной деятельности экспериментальные или не урегулированные законом способы осуществления хозяйственной деятельности. В частности:

- применять смарт-контракты для осуществления некоторых хозяйственных операций;

- заключать с третьими лицами договоры конвертируемого займа;

- заключать соглашения о предоставлении опциона и опционные договоры;

- осуществлять оборот электронных денег, открытие электронных кошельков;

- использовать криптовалюты в международных сделках, выступать в качестве операторов криптовалютных бирж и операторов обмена криптовалют.

Очевидно, что резиденты ПВТ обладают огромным количеством преференций. ПВТ является своеобразным экспериментальным проектом, в рамках которого проверяются и тестируются будущие модели для проверки их потенциального эффекта при последующем внедрении в экономику.

Учитывая потенциальную возможность использования указанного режима для формирования лжепредпринимательских структур или организаций, нацеленных в первую очередь на минимизацию налоговых отчислений, для резидентов ПВТ закреплены ряд дополнительных обязательств. Так, резиденты ПВТ обязаны:

- ежегодно проводить обязательный аудит годовой бухгалтерской (финансовой) отчетности;

- ежегодно представлять в Администрацию ПВТ отчет о деятельности;

- вести отдельный учет выручки (доходов) и затрат (расходов), относящихся к каждой из категорий осуществляемой деятельности (операций);

– получать заключение внешнего аудита по проектам, предусматривающим создание, размещение или иное использование цифровых знаков (токенов).

Также резиденты ПВТ обязаны информировать Администрацию и налоговый орган по месту постановки на учет о движении денежных средств по счетам, открытым резидентом ПВТ в банках и иных кредитно-финансовых организациях, созданных в соответствии с законодательством иностранного государства, с местом нахождения за пределами Республики Беларусь, а также о движении электронных денег по электронным кошелькам.

Иными словами, резидент ПВТ должен отчитываться о своих производственных цепочках и движении денежных средств. Данное требование видится справедливым, так как налоговые преференции являются крайне привлекательными и, соответственно, должны быть направлены на решение задач и достижение целей по разработке инновационных продуктов.

Как свидетельствует практика, опыт Республики Беларусь является положительным, что подтверждается ростом резидентов, экспортной выручки, количеством привлеченных инвестиций. Поэтому срок действия правового режима ПВТ продлен до 1 января 2049 г.

Республика Беларусь продемонстрировала, что создание специальных правовых режимов для привлечения инвестиций в область высоких технологий является успешной моделью экономического развития. Можно согласиться с высказыванием Абрамяна, о том, что «данная модель показывает, что чем больше ресурсов вкладывается в стимулирование инвестиционно-инновационной деятельности в контексте развития цифровой экономики на территории региона, тем больше инвестиций это привлечет в региональную экономику в будущем как результат роста инвестиционной привлекательности ввиду повышения качества информационно-коммуникационной инфраструктуры» [5].

Таким образом, успешный опыт Республики Беларусь в вопросе создания и последующего функционирования специальной экономической зоны (режима) развития высокотехнологичных проектов заслуживает особого внимания. Вместе с тем целесообразно не останавливаться на достигнутом и, опираясь на накопленный опыт, продолжить процесс разработки и создания правовых режимов для их последующего внедрения в практику других государств с целью повышения их инвестиционной привлекательности, в том числе и применительно к размещению в них предприятий инновационных информационно-коммуникационных технологий.

Список литературы

1. О развитии цифровой экономики : Декрет Президента Респ. Беларусь, 21.12.2017, № 8 / Нац. центр правовой информ. Респ. Беларусь // ЭТАЛОН. Законодательство Республики Беларусь – Минск, 2018.
2. О Парке высоких технологий: Декрет Президента Респ. Беларусь, 22.09.2005, № 12: в ред. Декрета Президента Респ. Беларусь от 21.12.2017 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2018.
3. Цифры и факты. URL: <https://www.park.by/http/facts/> (дата обращения: 16.08.2022).

4. Государство и право в XXI веке: материалы международной научно-практической конференции, посвященной 95-летию юридического факультета Белорусского государственного университета, 26–27 ноября 2020 г., г. Минск / БГУ, Юридический фак.; [редкол.: Т. Н. Михалёва (гл. ред.) и др.]. Минск: БГУ, 2021. С. 491–495.

5. Бизнес. Образование. Экономика: междунар. науч.-практ. конф., Минск, 1–2 апр. 2021 г.: сб. ст. / редкол.: В. В. Манкевич [и др.]. Минск: Институт бизнеса БГУ, 2021. С. 125–128.

6. Кадацкая Д. В., Лаврова Ю. С. Сквозные технологии в эпоху цифровой экономики как фактор формирования инновационной предпринимательской среды // Modern Economy Success. 2020. № 2. С. 94–99.

В. К. Сабирова,

доктор филологических наук, профессор,
Ошский государственный университет

Г. З. Абытова,

кандидат филологических наук, старший преподаватель,
Ошский государственный университет

А. А. Умарова,

преподаватель, Ошский государственный университет

А. Айзирек,

Ошский технологический университет

СМИ ЮЖНОГО РЕГИОНА НА РУССКОМ И КЫРГЫЗСКОМ ЯЗЫКАХ И ИХ РОЛЬ В ВОСПИТАНИИ МОЛОДЕЖИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В статье представлен краткий обзор роли русскоязычных и кыргызскоязычных СМИ, имеющих право издаваться на юге Кыргызской Республики, несмотря на различного рода нюансы, связанные со сменой владельца или приходом новой команды журналистов в коллектив редакции и т. д. При этом дается аналитическое обобщение их содержательного и развивающего контента, имеющее целью показать «лицо», т. е. сущность данного печатного издания, с акцентом на вопросы права в цифровой сфере.

Ключевые слова: контентный облик, масс-медиа, молодежь, право, содержание, цифровизация

THE MASS MEDIA OF THE SOUTHERN REGION IN RUSSIAN AND KYRGYZ LANGUAGES AND THEIR ROLE IN EDUCATING YOUNG PEOPLE IN THE CONDITIONS OF DIGITALIZATION

Abstract. This article provides a brief overview of the role of Russian-language and Kyrgyz-language media that have a place to be and the right to be published in the south of the Kyrgyz Republic, despite various nuances associated with a change in ownership or the arrival of a new team of journalists in the editorial team, etc. At the same time, an analytical generalization of their meaningful and developing content is given, which

aims to show the “face”, i. e. the essence of this print publication, with a focus on legal issues in the digital sphere.

Keywords: Content image, Mass media, Youth, Right, Content, Digitalization

Бурный культурно-политический процесс и всем известные общественно-экономические перемены, связанные с коронавирусной пандемией в мире, в Кыргызской Республике, как и во всем мире, создают объективные трудности для представителей современной молодежи в поисках жизненного пути. В связи с этим необходимо обращать пристальное внимание на сферу молодежной политики, особенно на юге Кыргызстана, широко известного как потенциально конфликтная зона. Это и межэтнические столкновения между узбеками и кыргызами в 1990, 2010 гг., и пограничные стычки между кыргызами и таджиками в 2014, 2020, 2022 гг., превратившиеся в обеспокоенность общества не только в этих странах, но и во всей Центральной Азии и целом мире. Развитие информационных технологий и научного подхода в решении жизненно важных проблем Кыргызстана как горной республики, богатой природными ресурсами – залог будущего социально-экономического успеха страны. Время от времени вспыхивают стихийные бунты местных жителей в местах добычи полезных ископаемых, куда прибывают инвесторы из Китая, России, Канады и иных стран. Порой многие из них выливаются в затяжные социальные кризисы, связанные с непопулярными у народа решениями властей.

Одним из приоритетных путей выхода из затянувшегося общественно-политического кризиса является привлечение и содействие интересу молодежи к различным образовательным программам, научно-исследовательским проектам и широким информационным компаниям посредством организации курсов, семинаров, налаживания широких международных связей с образовательными центрами республики и стран ближнего и дальнего зарубежья. И в этом плане неоценимую помощь могут и должны оказать средства массовой информации (СМИ).

Молодежь, особенно студенчество вузов юга Кыргызстана, или работающая в древнем городе Ош, сталкивается с необходимостью самостоятельного существования в цифровом обществе. Не имея навыков полноценной жизнедеятельности, твердых убеждений, коммуникативных навыков, способности отстаивать свою позицию, они часто попадают под влияние чужого мнения. Большинство житейских ситуаций, приводящих к таким личным трагедиям, как приобщение к алкоголю, табакокурение, наркотики, нежелательная беременность, ранние (детские) браки, суицид, приносящие непоправимый вред здоровью, случаются в силу неумения противостоять чужому давлению, влиянию ложного общественного мнения, навязанных телевидением и другими СМИ стереотипами.

К сожалению, молодые люди понимают право на самостоятельность как вседозволенность, необходимость испытать все запретное. Это говорит не столько об отсутствии воспитания, сколько о незнании молодежью элементарных правил безопасной жизнедеятельности. В целом молодежь вооружена различными наставлениями, советами родителей и родственников о вреде алкоголя, курения, средствах предохранения, но это не дает должного эффекта. Государственные программы направлены на борьбу со следствием и ориентированы на имеющих проблемы людей,

а не на предупреждение негативных ситуаций. Тем более идеи вседозволенности льются из Интернета.

Причина социальных опасностей, в которых оказываются молодые люди, в том, что они не обладают навыками живого общения, не умеют анализировать собственные поступки, руководствуются надуманными понятиями о дружбе, самостоятельности, престиже. В реальной максималистски настроенной среде молодежи с определенной субкультурой, часто возникает необходимость быстро принимать нужные решения, которые не должны вредить его положению в среде друзей. Пристрастие и пагубные привычки возникают в силу неумения молодежи противостоять советам, просьбе, насмешкам друзей, сокурсников, просто незнакомых людей. Цифровая среда создает иллюзию их полной свободы, внушая им право на совершение различных проступков.

Необходимо обучать студентов и остальную молодежь конкретным навыкам, позволяющим им общаться с друзьями, избежать тупиковых ситуаций, приносящих вред их здоровью. В газетных статьях, радио и телевизионных передачах, в материалах электронных СМИ нужно ставить проблемы, взятые из жизни и связанные с этическим выбором, студенты должны решать вопросы, с различными вариантами ответов и прорабатываются различные возможности и результаты выхода из этих трудных жизненных ситуаций. Необходимо сейчас в цифровой среде развивать контент культурных программ, в том числе на местных языках именно для детей и молодежи.

Разработка различного рода просветительских программ, которые должны пропагандироваться, в основном, через социальные сети и СМИ диктуется стремлением не кардинально решить социально-экономические проблемы, а в меру своих способностей и в рамках законодательства повлиять на качественное улучшение психологического и социального здоровья молодежи путем обучения их конкретным навыкам решения проблем житейских ситуаций, предупреждения от вышеперечисленных социальных опасностей.

В нашем случае под потенциальными силами общества, которому завтра превращать в жизнь все намеченное старшими поколениями, мы понимаем студенчество и молодежь, которые представляет собой достаточно самостоятельную социальную структуру. Как известно, никто не знает собственные проблемы, лучше, чем он сам. Необходимо обозначить и выявить круг и особенности проблем, но именно молодежь будет выступать главным инициатором и индикатором стоящих перед ними проблем, задач и трудностей. Часто решение тех или иных проблем требует не просто финансовой помощи, а моральной поддержки, одобрение группы, сокурсников, а главное, изменение общественного мнения по отношению к тому или иному проступку или ошибке. Эффективность Тик-Тока, Whats upp, Telegram и иных социальных сетей налицо, ведь размещая многочисленные материалы о семейном насилии в современном обществе, очевиден и пропагандистский эффект от этих материалов по принципу, если так делают, значит, и мне можно. В связи с этим вспоминается также такой факт, когда появился «казанский стрелок», расстрелявший учителей и учеников в собственной школе. Что это, как не проявление такого прецедента, когда в западных странах

такое возможно и время от времени в СМИ появляются такого рода трагические сообщения.

Всегда необходимо стремиться к формированию толерантности к чужим ошибкам, стремлению к солидарности и взаимопомощи, повышению чувства ответственности к своим поступкам, способности отстаивать собственное мнение и держаться в обществе с достоинством.

По результатам небольшого социологического опроса среди молодежи, включавшего такие вопросы, как «Какие СМИ вам предпочтительны?», «Кто из журналистов вам знаком и импонирует его подача материала?», «Что вы читаете из современной прессы?», «Нужно ли СМИ вмешиваться в политику?», «На каком языке вы смотрите телепрограммы или слушаете радиопередачи?», были получены весьма любопытные результаты.

На вопрос: «Какие СМИ вам более предпочтительны?» были ответы, отражающие способ и вид передачи материала в СМИ («телевизионные», «радио», «пресса», «Интернет»), обозначающие страну или место выпуска СМИ (Россия, Казахстан, Узбекистан, Бишкек, Ош – в порядке убывания интереса) или тип подачи материала (информационный, аналитический, развлекательный, обучающий, разный).

Вопрос «Кто из журналистов вам знаком и импонирует ли вам его подача материала?» вызвал самые разные ответы, названы фамилии зарубежных, российских журналистов, а также республиканских и местных СМИ.

При ответе на вопрос «Что вы читаете из современной прессы?» молодые люди отвечали: «новости о коронавирусе», «политические новости», «спортивные сообщения», «новое из области музыки и эстрады». Характерно, что почти никто не интересовался вопросами экономики и внешней политики.

Однозначен был ответ на вопрос, который, наверняка даже не стоит задавать после событий 4 октября 2020 г.: «Нужно ли СМИ вмешиваться в политику?» Единогласный ответ у всех опрошенных – «Да», что свидетельствует о больших потенциальных возможностях СМИ в области молодежной политики в нашей республике в трансформационный период, отягощенный последствиями пандемии.

Интересно, что вопрос «На каком языке вы смотрите телепрограммы или слушаете радиопередачи?» также почти не вызвал разногласий в том смысле, что большинство молодежи смотрят и слушают передачи по ТВ и РВ на русском языке, предпочитая его кыргызскому, узбекскому и иным языкам. Хотя многие молодые люди ходят на языковые курсы английского, немецкого, корейского, китайского, итальянского, испанского и других языков, ставя перед собой цель уехать поработать в страну иного языка, а может быть, и навсегда.

Характерным фактом является то, что после каждого политического кризиса националисты разыгрывают языковую карту, стремясь убрать из Конституции статус официального у русского языка.

Отсюда следует, что как и кыргызскоязычные в виде газеты «Супер-Инфо», сайта «Турмуш» и иных топовых медийных продуктов, так и русскоязычные СМИ на юге Кыргызстана имеют определенный вес, играют важную роль в освещении общественно-политических событий региона и имеют опыт, возможности, ресурсы для взаимоподдержки, взаимодействия с иноязычными СМИ.

Сделанный обзор газет «Нур», «Дидактика», «Умут-ТВ», «ЭлТР», «Ынтымак», «Нур-ТВ», «Ош-ТВ», «Ош-пирим», которые были основаны за последние два-три десятка лет, показывает, что они выходят на русском, узбекском и кыргызском языках и предназначены для молодежи (студентов и неучащейся молодежи), а также иных возрастных групп.

Это предполагает билингвизм учащейся молодежи, в основном студентов, и придает газетам, телевидению, радио, Интернет и социальным сетям свой оригинальный колорит. Примечательно еще и то, что материал для подачи в масс-медиа, обработку поступающей информации, интервью, репортажи, фотоэтюды и т. д. осуществляют журналисты с активной жизненной позицией, желающие самоутвердиться. В целом, это выпускники языковых факультетов (факультеты русской и кыргызской филологии) и отделения журналистики.

На первых страницах или начальных кадрах во всех печатных и электронных СМИ подается самый важный материал: значительные общественные, политические, культурные события города Ош, страны и всего мира. На второй и следующих страницах освещаются общественные, научные мероприятия, идут различные обзоры культурных, спортивных событий и их аналитика, актуальные интервью. Даются материалы научно-популярного характера, материал для расширения кругозора, психологические тесты, результаты социологических опросов и исследований, проводимых различными организациями. Преобладают материалы о вреде наркомании, табакокурения, увлечения спиртными напитками, о последствиях ранних браков и нежелательной беременности (статьи «Алкоголь бардык олчомдо зыяндуу», «Тамекин менен тамыран калгыр», № 10 (79) за декабрь); интервью с интересными для молодежи личностями (артистами, преподавателями, деятелями искусства и науки, например, интервью с видными учеными «Невозможное возможно...» в № 2 (89) за февраль). Последние страницы газет и кадры радио и телепередач, как принято, развлекательного характера: читателям и зрителям предлагаются головоломки, кроссворды, сканворды, гороскоп, тексты популярных песен, различного рода конкурсы, фотоюмор и др.

Таким образом, можно прийти к выводу, что СМИ юга Кыргызстана, особенно русскоязычные и кыргызскоязычные, играют большую роль в воспитании молодежи, освещая проблемы алкоголизма, наркозависимости, насилия, табакокурения, проституции, ранних браков, психологических стрессов при общении с другими людьми, публикуя ответы на их вопросы, интервью с видными врачами-наркологами, юристами, психологами, с людьми старшего поколения, которые могут дать полезный совет в данных ситуациях или с людьми, имевшими горький опыт по данным проблемам. Также они содействуют расширению кругозора молодых людей путем публикаций научно-популярных статей, снятию психологического стресса, и, что нужно особенно отметить, содействуют защите прав и интересов молодежи, распространяя информацию общего и развивающего характера. Нужно обратить особое внимание на вопросы права, поскольку сегодняшняя образовательная среда, пережившая онлайн-обучение в период пандемии, еще раз доказала факт большей эффективности службы работников современного образования в цифровой среде, в частности по вопросам прав молодежи.

Список литературы

1. Гридчин М. М. Проблемы влияния информационных технологий на молодежь // Власть. 2007. № 9.
2. Запекина Н. М. Современная досуговая периодика для детей: тематико-типологические черты // Вестник Челябинской государственной академии культуры и искусств. 2018. № 2.
3. Золотов Е. А. Воздействие аудиовизуального насилия на подрастающее поколение России: историко-культурологический аспект // Электронный журнал «Знание. Понимание. Умение». 2018. № 4.
4. Влияние СМИ на молодежь // Медиаобразование: от теории – к практике / сост. И. В. Жилавская. – Томск: Изд-во Томск. ин-та инф-ных технологий, 2012.
5. Молодое поколение и телевидение (результаты и выводы из исследования в Краснодарском крае) / О. Н. Никитина, С. Н. Лыкова, Е. А. Таскина, Ю. С. Ночевная. – Краснодар, 2018.
6. Панов С. «Интернет-зависимость»: причины и последствия // Учитель. 2018. № 5.
7. Рогозянский М. Э. Воспитательный потенциал телевидения: теоретические вопросы, осмысленные практиком // Образование и общество. 2018. № 2.
8. Сандалова К. Воспитание «Хулигана «Молотком»: чему учат молодёжные журналы? // Москва. 2006. № 3. С. 164.
9. Федоров А. В. Отношение учащихся к насилию на экране, причины и следствия их контакта с экранным насилием // Педагогическая диагностика. 2007. № 4. С. 138.
10. URL: <https://cyberleninka.ru/article/n/duhovno-nravstvennoe-vozpitanie-molodezhi-cherez-smi> (дата обращения: 26.08.2022).

И. В. Сабодах,

кандидат физико-математических наук, доцент,
Сибирский федеральный университет

Д. А. Давыдова,

магистрант,

Институт управления бизнес-процессами,
Сибирский федеральный университет

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ДЛЯ РАССЛЕДОВАНИЯ ИСКАЖЕНИЯ ФИНАНСОВЫХ ПОКАЗАТЕЛЕЙ КОМПАНИИ

Аннотация. Анализируя финансовую отчетность и ее показатели на предмет фальсификации, можно не только избежать необоснованных решений, но при этом и сэкономить финансовые ресурсы компании, а также определить ее сильные и слабые стороны. Главенствующую роль в этой теме играет система внутреннего контроля и внедрение цифровых технологий во все процессы компании. В статье представлены финансовые показатели, на основании которых определяется фальсификация финансовой отчетности, а также приведены преимущества и обоснована важность использования цифровых технологий компаниями для установления данного факта.

Ключевые слова: цифровые технологии, финансовая отчетность, финансовые показатели, фальсификация, цифровая экономика, цифровая трансформация

USING DIGITAL TECHNOLOGY TO INVESTIGATE THE COMPANY'S FINANCIAL MISSTATEMENTS

Abstract. By analyzing the financial statements and its indicators for falsification, you can not only avoid unreasonable decisions, but also save the company's financial resources, as well as determine its strengths and weaknesses. The main role in this topic is played by the internal control system and the introduction of digital technologies into all processes of the company. The article presents the financial indicators on the basis of which falsification of financial statements is determined, as well as the advantages and substantiation of the importance of using digital technologies by companies to establish this fact.

Keywords: Digital technology, Financial reporting, Financial performance, Falsification, Digital economy, Digital transformation

На сегодняшний день актуальной проблемой является фальсификация финансовой отчетности, которая включает в себя риски связанные как с инвесторами, так и кредитора. Искажения данных бухгалтерской отчетности могут оставаться необнаруженными по некоторым причинам, к которым можно отнести как не применения современных методов и методологии финансового и бухгалтерского учета, в зависимости от анализируемых данных отчетности компании, так и с противоречиями в законодательстве и нормативно-правовом регулировании. Переход к цифровым технологиям в экономике, бизнесе и социальной сфере порождает необходимость их правового регулирования.

Мошенничества в финансовой отчетности определяется как некоторые действия, которые приводят к искажению реальных данных финансовых отчетов с целью фальсификации данных отчетов, ведущие к завышению прибыли, завладению имущества принадлежащего компании и, как правило, совершаются такие действия руководителем компании. Таким образом, возрастает актуальность преобразования системы внутрикорпоративного управления в компании с целью своевременного установления факта мошенничества и его предотвращения в финансовой и бухгалтерской отчетности.

Одним из методов оценки состояния компании является анализ финансовых показателей, благодаря которым можно выделить сильные и слабые стороны компании и сформировать в дальнейшем ее стратегию развития, что является основополагающим стратегического планирования компании. Данный метод оценки реализуется ради определения актуального и оптимального курса достижения главной цели, которую преследует компания, например, увеличение прибыли, повышение финансовой устойчивости, обеспечение ликвидности компании и т. д.

Известны более двухсот показателей в финансовом мире, которые можно использовать при анализе финансовых показателей, которые затрагивают основные стороны деятельности компании, к ним относятся такие показатели как чистая прибыль, рентабельность активов и собственного капитала, текущая ликвидность

и так далее, для которых рассчитываются свои коэффициенты с использованием соответствующих формул, присущих конкретному показателю.

Приведем основные показатели финансовой деятельности, которые могут быть использованы при расследовании искажения финансовой и бухгалтерской отчетности:

- темп роста качества активов – если значение индикатора больше единицы, компания увеличивает долю внеоборотных активов в совокупном объеме активов;
- темп роста выручки, темп снижения доли маржинального дохода в выручке – показатели, которые могут быть задействованы для мошенничества с выручкой от продаж;
- темп роста доли расходов в выручке от продаж – не должен существенно отличаться от темпов роста продаж;
- темп роста оборачиваемости дебиторской задолженности – данный индикатор должен находиться в пределах одного значения в условиях стабильного роста бизнеса;
- темп роста финансового рычага – рыночная стоимость акций зависит от данного показателя;
- темп роста доли амортизационных отчислений – данный показатель должен быть равен единице.

Проведя анализ показателей финансовой и бухгалтерской отчетности на предмет искажения и фальсификации данных, можно минимизировать, либо нейтрализовать, риски принятия управленческих решений, а, как следствие, сохранить денежные и трудовые ресурсы.

Системам внутрифирменного контроля и вводу цифровых технологий во все процессы компании с последующим их использованием отводится все большее внимание, так как фальсификацию и факт мошенничества в финансовой и бухгалтерской отчетности лучше предотвратить своевременно для минимизации негативных последствий для самой компании.

Цифровые технологии становятся неотъемлемой частью всех бизнес процессов компании, которые ставят перед собой цель достижения максимальной прибыли с учетом имеющихся ограниченных ресурсов.

Для более совершенного использования информации финансовые отчеты должны обрабатываться несколькими методами и способами. Однако, возникает вопрос – способна ли технологическая мощь не только эффективно контролировать, но и работать с предоставленными финансовыми данными?

Цифровые технологии трансформируют операционную модель предприятия, т. е. порядок и методы применения корпоративной стратегии в повседневной деятельности, а также повышают степень эффективности инвестиций и помогают выявить уникальные ранее неизвестные возможности на рынке [2].

Представим на рис. 1 основные направления, оказывающие в той или иной степени влияние цифровизации экономики на формирование финансовой и бухгалтерской отчетности компаний [1].

Таким образом, цифровизация экономики играет важную роль и оказывает существенное воздействие на процесс формирования и использования финансо-

вой и бухгалтерской отчетности, в том числе и в аспекте установления фальсификации данных, отраженных в анализируемой отчетности.

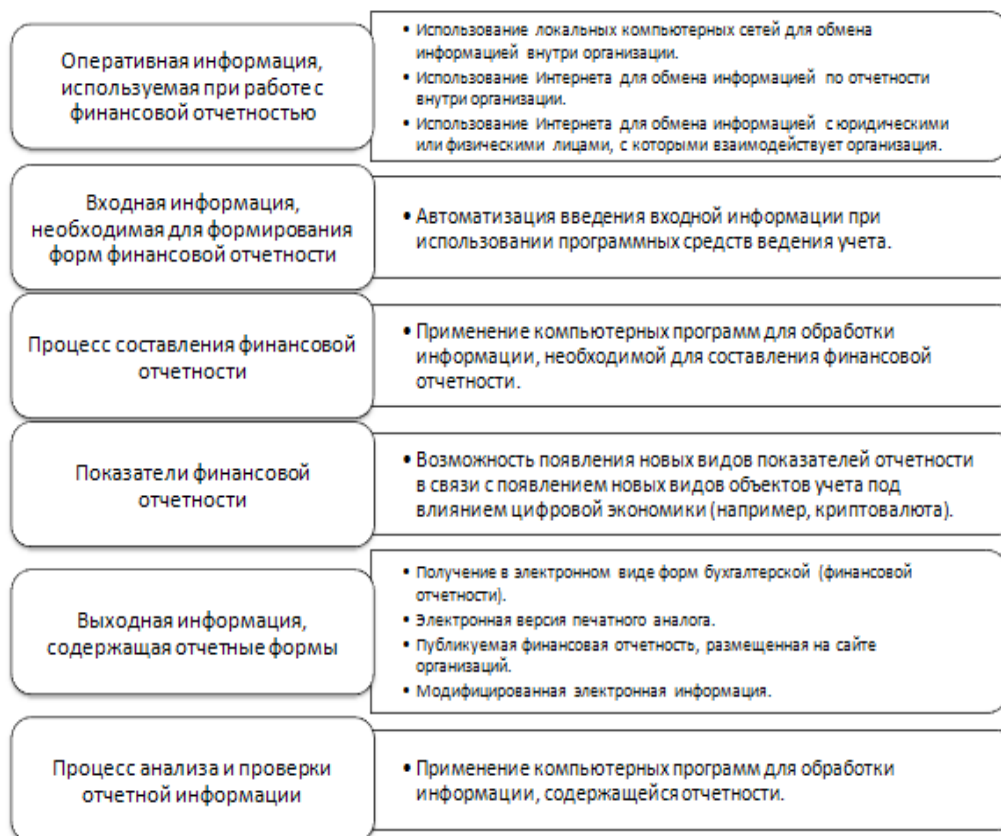


Рис. 1. Влияние цифровизации экономики на состояние финансовой отчетности

На пути к формированию цифровой экономики происходят технологические взрывы, под которыми понимается «комбинация технологий, дающая возможность создавать новые продукты и сервисы, которые, с одной стороны, формируют новые сферы деятельности, а с другой – радикально изменяют существующие отрасли экономики» [3].

Приведем примеры цифровых технологий: Big Data (большие данные), искусственный интеллект, корпоративный Интернет, компоненты робототехники и RPA (роботизированная автоматизация процессов), XBRL, блокчейн и тому подобные, в основе которых используются современные цифровые технологии и методы обработки данных.

Современные цифровые технологии, вызывающие стремительный рост потоков данных, все чаще становятся базой для сложных общественных структур и отношений, так как они делают основой формирование нового типа экономики. Этому типу свойственны отношения в сфере производства, обработки, анализа и передачи данных.

Многие компании инвестируют в цифровые технологии, так как ожидают положительного влияния цифровизации на текущую деятельность своей компании.

Цифровая трансформация реализуется по определенным причинам, к которым можно отнести тот факт, что современный бизнес использует современные технологии, которые могут обрабатывать большие объемы данных финансовой и бухгалтерской отчетности, также методы анализа показателей финансовой отчетности позволяют своевременно, точно и достоверно собирать, обрабатывать, анализировать и использовать полученные данные, при этом реализуется принцип быстрого доступа к финансовой информации компании и, как следствие, компании меняют свои бизнес стратегии и модели, с целью использования преимуществ цифровой трансформации в своей финансово-экономической деятельности.

Таким образом, цифровая экономика становится ведущим сегментом, драйвером роста и развития экономической системы в целом.

Список литературы

1. Бабкин А. В., Буркальцева Д. Д., Пшеничников В. В., Тюлин А. С. Криптовалюта и блокчейн-технология в цифровой экономике: генезис развития // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2017. Т. 10, № 5. С. 9–22.
2. Мельник М. В. Модернизация учетно-контрольных и аналитических процессов в условиях цифровой экономики // Учет. Анализ. Аудит. 2018. № 3. С. 129–130.
3. Сухарева М. А. От концепции постиндустриального общества к концепции экономики знаний и цифровой экономики: критический анализ терминологического поля // Государственное управление. Электронный вестник. 2018. № 68. С. 445–464.

Д. В. Савлаев,

магистрант,

Российский государственный университет
нефти и газа имени И. М. Губкина

ЦИФРОВЫЕ ТЕХНОЛОГИИ КАК МЕХАНИЗМ ПОВЫШЕНИЯ ОБЪЕМОВ ЭКСПОРТА РОССИЙСКИХ ТОВАРОВ

Аннотация. Промышленная революция 4.0, сформировавшаяся в начале XXI в., привела российскую экономику к цифровой трансформации и внедрению ИИ и цифровых платформ для увеличения качества ведения бизнеса. Цифровые технологии тесно связаны со всеми сферами государственного управления, сферой финансов и экономики. Научная новизна работы заключается в поиске и оптимизации внедрения новых цифровых платформ, улучшающих основные и второстепенные задачи торговли на международном рынке. Основной целью исследования является выяснение реального влияния цифровых платформ на обеспечение качества деятельности торговых компаний и их вклад в увеличение экспорта. В рамках исследовательской работы выполнены следующие задачи: поиск основных цифровых платформ, анализ статистических данных повыше-

ния и уменьшения ввозимого экспорта, выявление основных изменений цифровой трансформации.

Ключевые слова: право, цифровые технологии, цифровизация регионов Российской Федерации, повышение экспорта, РЭЦ, цифровые платформы, цифровая трансформация

DIGITAL TECHNOLOGIES AS A MECHANISM TO INCREASE EXPORTS OF RUSSIAN GOODS

Abstract. The Industrial Revolution 4.0, which took shape at the beginning of the 11th century, led the Russian economy to digital transformation and the introduction of AI and digital platforms to increase the quality of business introduction. Digital technologies are closely connected with all areas of public administration, finance and economics. The scientific novelty of the work lies in the search and optimization of the introduction of new digital platforms that improve the main and secondary tasks of trading in the international market. The main goal of the study is to find out the real impact of digital platforms on ensuring the quality of the activities of trading companies and their contribution to increasing exports. As part of the research work, the following tasks were completed: search for the main digital platforms, analysis of statistical data on the increase and decrease in imported exports, and identify the main changes in digital transformation.

Keywords: Law, Digital technologies, Export, REC, Digital platforms, Digital transformation

В настоящее время большинство российских компаний передают ряд своих полномочий и обязанностей на аутсорсинг с целью улучшить транспортно-логистические процессы и обеспечить безопасность цепочек поставок. Это, в свою очередь, приводит к проблемам осуществления контроля выполнения поставленных логистических задач. Для решения этой проблемы отечественные компании внедряют «сквозную отслеживаемость» для наблюдения за этапами доставки от производителя до потребителя.

Функция end-to-end представляет собой процесс контроля за передвижением товаров. Сервис помогает экспортерам анализировать пути перевозки. Самостоятельно выстроить систему обработки данных покупателя и продавца, наладить процессы с изменением этапов поставки. Также сквозная отслеживаемость выполняет одну из самых важных задач по выстраиванию и внедрению цифровых систем, которые обеспечивают безопасную и быструю обработку новых заказов. Цифровые технологии собирают в себе все преимущества инструментов современной экономики, поскольку открывают перед производителем доступ к цифровым платформам, что значительно улучшает качество ведения бизнеса.

Трансформация российской цифровой экономической деятельности стремительно развивается, так, министром промышленности и торговли РФ Денисом Мантуровым был разработан проект «Международная кооперация и экспорт» на период с 2019–2024 годы. Задачами проекта стали увеличение объема экспорта

в области энергетических товаров, а также продукции машиностроения, совершенствование обрабатывающей промышленности и сельского хозяйства, разработка улучшенной системы разделения труда, а также увеличение объема товарооборота между государствами Евразийского экономического союза. Важным событием стало создание цифровой платформы «Мой экспорт» в рамках проекта.

Сервисы платформы «Мой экспорт» решают множество задач на всех этапах экспортного оборота, субсидии на транспортировку. Платформа позволяет на первом этапе провести полный анализ и помочь в поиске покупателя. До конца все функции не представлены из-за ранней стадии платформы. В своем обращении Вероника Никишина, генеральный директор Российского экспортного центра, высказалась о масштабной доработке платформы в области переноса всей работы с документами на цифровой вид. На портале «РЭЦ» также представлены и другие не менее важные цифровые разработки, которые нацелены на улучшение качества ведения бизнеса. Интерактивная система «Навигатор» дает возможность проанализировать и выявить требования внутренних и внешних рынков по критериям: наименование продукта, страна, вид меры. Одной из важных функций системы является поиск информации по ставкам ввозных таможенных пошлин в отношении зарубежных стран и экспорта российской продукции.

Разработана программа по оптимизации логистических маршрутов 1С:TMS, которая помогает пользователю учитывать все факторы при перевозке грузов, такие как габариты груза, характеристики, технические особенности груза. Инструменты программы позволяют создать пошаговую инструкцию по перевозке груза, выстроить маршрут, выписывать путевой лист, создавать задания в АРМ водителя. Благодаря сервисам такого рода растет товарооборот по всей стране.

Цифровые технологии берут на себя все больше и больше задач, связанных с упрощением создания капитала и улучшением работ по управлению в компаниях. Главенствующим направлением в создании дружественных отношений между странами является экспорт продукции. С помощью цифровых технологий у компаний появится возможность увеличить рост экспортируемой продукции как качественно, так и количественно.

Использование цифровых технологий в области топливно-энергетических товаров за первый квартал 2022 г. увеличилось в полтора раза по сравнению с 2021 г. Нефтегазовая отрасль является основной экспортной продукцией России, которая заняла больше половины всего экспорта за 2022 г., его объем составил 63 % всего экспортируемого груза, что также превышает поставляемый товар за 2021 г. в этой области на 10 %. Также выросла доля экспорта изделий из металлов: по сравнению с 2021 г. в 2022 г. она увеличилась на 2 % и составила 12 %. Показатели увеличения роста экспортной продукции в химической промышленности, продовольственных товаров, машин и оборудования растут, как за счет отечественных специалистов логистики, разработки, управления, так и за счет надлежащего выполнения поставленных задач цифровым технологиям.

Экосистема цифровой транспортной логистики предоставляет доступ к интерактивным веб-технологиям, с помощью которых можно напрямую подключаться к транспортно-складской системе, планировать ресурсы предприятия, осуществ-

влять любые виды взаимодействия с контрагентами (поставщиками, посредниками, потребителями).

В этом случае информационный поток опережает процесс доставки, т. е. не выступает производным от материального потока, а является основным потоком в транспортно-логистической системе. После подключения к услуге пользователь сможет рассчитать стоимость перевозки товара, сразу же отправить заявку на организацию доставки товара и последующий контроль процесса перевозки как внутри страны, так и за ее пределами. Технология отслеживания цепочки поставок помогает быстро реагировать на изменения, позволяя заинтересованным пользователям, в том числе поставщикам, логистическим операторам, потребителям, принимать меры и изменять спрос, перенаправлять материальный поток и реагировать на любые изменения в цепочке поставок. Интеграция инструментов и систем цифровой отслеживаемости позволяет различным звеньям цепочки поставок получать точную информацию о текущих запасах, поступающих заказах и товарах, находящихся в пути, в режиме реального времени.

Выявление полезных цифровых платформ позволит российским компаниям упростить пути доставки товаров, открыть новые способы поиска товаров и покупателя, значительно поможет компаниям анализировать продукцию, находить покупателя.

Список литературы

1. Абдрахманова Г. И. Индикаторы цифровой экономики: 2017: статистический сборник. Москва: НИУ ВШЭ, 2017. 250 с.
2. Ассоциация автоматической идентификации GS1. 2019. URL: <http://www.gs1ru.org>
3. Дмитриева Н. Е., Жулин А. Б., Артамонов Р. Е., Титов Э. А. Оценка цифровой готовности населения России: доклад к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества. Москва, 2021. 86 с.
4. Капранова Л. Д. Цифровая экономика в России: состояние и перспективы развития. Москва, 2018. 110 с.
5. Гохберга Л. М. Тенденции развития интернета: от цифровых возможностей к цифровой реальности: аналитический доклад. Москва, 2021. 274 с.
6. Распоряжение от 28.07.2017 № 1632 р «Об утверждении программы „Цифровая экономика Российской Федерации”» / Правительство России. URL: <http://government.ru/docs/28653/>
7. Шуйский В. П. Цифровизация мировой экономики и структура российского экспорта услуг. Москва, 2020. 10 с.
8. Verhovnik J., Duh E. S. The importance of Industry 4.0 and digital transformation for SMEs // *Elektrotehniški Vestnik*. 2021. Vol. 88, № 3. Pp. 147–149.
9. Zuti B. Digitalization, regional competitiveness and the governments of the future // 3rd International young researcher scientific conference. Gödöllő, 2018. Pp. 396–403.

А. Л. Семенихин,
доктор военных наук, кандидат экономических наук, профессор
Санкт-Петербургский имени В. Б. Бобкова
филиал Российской таможенной академии

ПРОБЛЕМЫ НАЛОГООБЛОЖЕНИЯ ЦИФРОВЫХ АКТИВОВ

Аннотация. Статья рассматривает ключевые проблемы налогообложения операций, связанных с цифровыми валютами и перспективные направления разрешения возникающих при этом правовых и экономических противоречий. Проведен текущий и ретроспективный анализ международного государственного регулирования операций, связанных с использованием цифровых валют и активов. Приводится статистика категорий держателей цифровых валют, а также характеристика типовых операций с ними.

Ключевые слова: цифровая экономика, криптовалюта, виртуальная валюта, цифровая валюта, налогообложение, волатильность, государственное регулирование

PROBLEMS OF TAXATION OF DIGITAL ASSETS

Annotation. The article examines the key problems of taxation of transactions related to digital currencies and promising directions for resolving the legal and economic contradictions that arise in this case. The current and retrospective analysis of the international state regulation of transactions related to the use of digital currencies and assets is carried out. Statistics of categories of holders of digital currencies, as well as characteristics of typical transactions with them, are provided.

Keywords: Digital economy, Cryptocurrency, Virtual currency, Digital currency, Taxation, Volatility, Government regulation

Появление криптовалют на рынке финансовых операций является прогрессивным шагом в развитие цифровых технологий. Данная тенденция напрямую коррелирует с Указом Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». Очередным шагом в этом направлении стало принятие Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Федеральный закон № 259-ФЗ «О цифровых финансовых активах...»).

При активном стремлении государства регулировать обращение цифровых валют в стране у криптообщества возникло достаточно много проблем как в сфере использования данных валют, так и в сфере налогообложения по операциям с ними. В связи с тем, что отсутствует достаточно понятное законодательное регулирование многие держатели цифровых валют рискуют попасть под санкции административного и уголовного законодательства. Что, в свою очередь, заставляет их скрывать совершение сделок и обменных операций.

Не маловажным фактором является тот факт, что держатели цифровых активов практически не защищены со стороны государства от мошеннических операций со стороны многочисленных посредников. В то же время, государство приняло реше-

ние о создании еще одной полноценной денежной единицы – цифрового рубля, но при этом нет достаточно четких понятий о других криптовалютах, находящимся с 2021 г. в обращении уже на легальных основаниях в нашей стране.

Проведенные социологические исследования по возрастному показателю держателей криптовалют показывают: что 9 % являются миллениалы (лица от 21 до 38 лет) при этом средним показателем является всего 4 %. Высокую степень желания владеть цифровыми активами продемонстрировали представители, так называемого, «Поколения Z» (лица в возрасте от 13 до 21 года) стремление приобрести данную валюту выразили около 26 % [4].

Было установлено, что около 72 % владельцев считают цифровую валюту как долгосрочный финансовый актив (накопление и сбережение), а для 28 % всего лишь платежное средство.

Повсеместное распространение цифровых валют создает значительные риски не только для их держателей, но серьезные угрозы стабильности как национальной, так и глобальной финансовой системы. К этому относится: непредсказуемая динамика волатильности курса, недобросовестность продавцов криптовалюты, граничащая с мошенничеством.

Опросы показывают, что порядка 75 % держателей цифровых валют боятся хакерских атак, с целью кражи их финансовых активов. Чуть ниже процент опасений высказывают владельцы биткоин – 68 %. И это несмотря на это рынок цифровых валют стремительно растет. На рис. 1 показан «портфель» предпочтений владельцев цифровых валют по состоянию на 2019 г. [4].

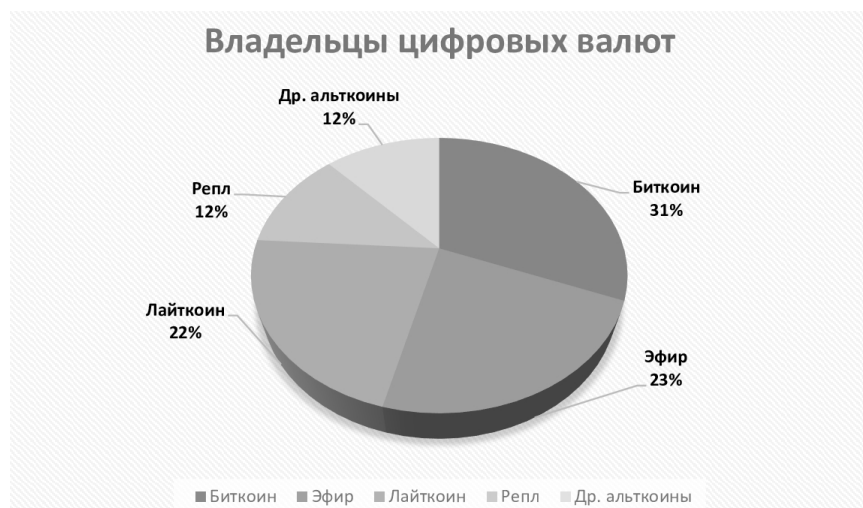


Рис. 1. «Портфель» предпочтений владельцев цифровых валют

Наиболее активно в цифровые валюты вкладывают зарубежные инвесторы (процент населения страны, владеющего криптовалютой):

- США – 17 %;
- Южная Корея – 22 %;
- Германия – 15 %;
- Россия – 2–9 %;
- остальные страны – 12 %.

В Российской Федерации, как показывают аналитические исследования, отношение к цифровым валютам сдержанно-осторожное. Проблемы, связанные с нерегулированием многих правовых аспектов, отталкивают подавляющее большинство потенциальных покупателей и владельцев данных видов валют (рис. 2).

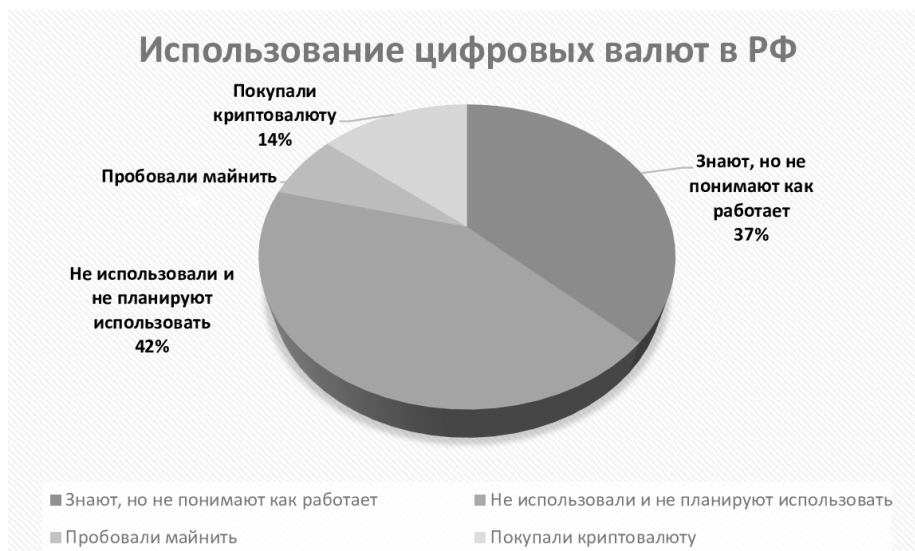


Рис. 2. Использование цифровых валют в Российской Федерации

Цифровые валюты это одно из «мест деятельности» хакеров. Пользуясь пробелами в законодательстве, совершают хищения и мошеннические действия. По данным Банка России до 2% криптовалют похищались с электронных кошельков их владельцев [6]:

2018 г. – 0,6 %;

2019 г. – 2,1 %;

2020 г. – 0,6 %.

При этом возможности защиты своих прав практически отсутствуют. Так на основании ст.14 Федерального закона № 259-ФЗ «О цифровых финансовых активах...» в судебном порядке можно оспаривать свои права лишь в том случае, если информировали о фактах обладания данной валютой или совершения сделок с ней в соответствии с НК РФ. Помимо этого, необходимо предоставить документы, подтверждающие владение цифровыми активами.

В свою очередь, в НК РФ отсутствует детально прописанное налогообложение сделок (оборота) цифровых активов. В этом случае применяются нормы, указанные в гл. 23 (НДФЛ), которые описывают базовые принципы взыскания налогов [3].

В России активно работают юридические и физические лица, занимающиеся майнингом цифровых валют (рис. 3). По оценкам специалистов, наша страна занимает в рейтинге третье место, уступая лишь США и Казахстану. Майнинг

распространен в регионах с низкой стоимостью электроэнергии, как правило в Сибирском федеральном округе, преимущественно в сельской местности.

Цифровые валюты не имеют четко выраженного национального характера, а по анонимности ее владельцев можно отнести к аналогу оффшорных зон, что и определяет низкую налоговую нагрузку. Поэтому первые попытки правового регулирования обращения цифровых валют рассматривались именно с точки зрения налогового администрирования, а не движения капиталов. На рис. 4–7 представлены варианты подходов к налогообложению [5].

Проведенный анализ показывает, что в Российской Федерации назрела необходимость создания специального законодательства, регулирующего оборот цифровых валют и прежде всего, с целью налогообложения. На наш взгляд, под налогообложение должны попасть следующие виды операций [2]:

- майнинг;
- оплата криптовалютой товаров, услуг и работ;
- обмен на фиатные валюты;
- хранение цифровых активов.

По оценкам экспертов потери бюджета Российской Федерации от оборота цифровых валют в 2021 г. составили примерно 140 млн долл. только от налога на прибыль, не учитывая иные операции с данными активами.

С 1 января 2021 г. были внесены в законодательство России изменения, которые закрепили понятие цифровых активов – «имущество». Исходя из этого, у владельцев криптовалют появилась обязанность подавать налоговую декларацию. Неуплата в течение трех лет НДФЛ при превышении 2.7 млн руб. может повлечь за собой привлечение к уголовной ответственности.

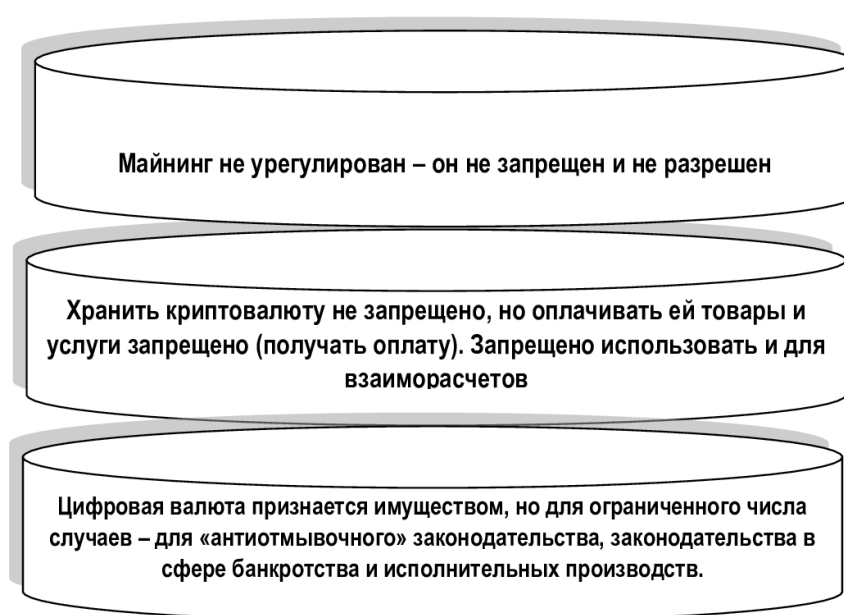


Рис. 3. Регулирование криптовалют в России

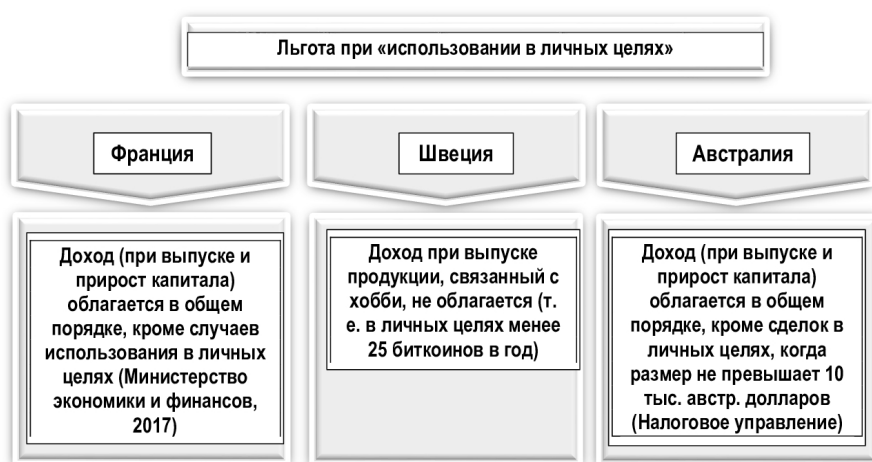


Рис. 4. Льготы для владельцев цифровых валют

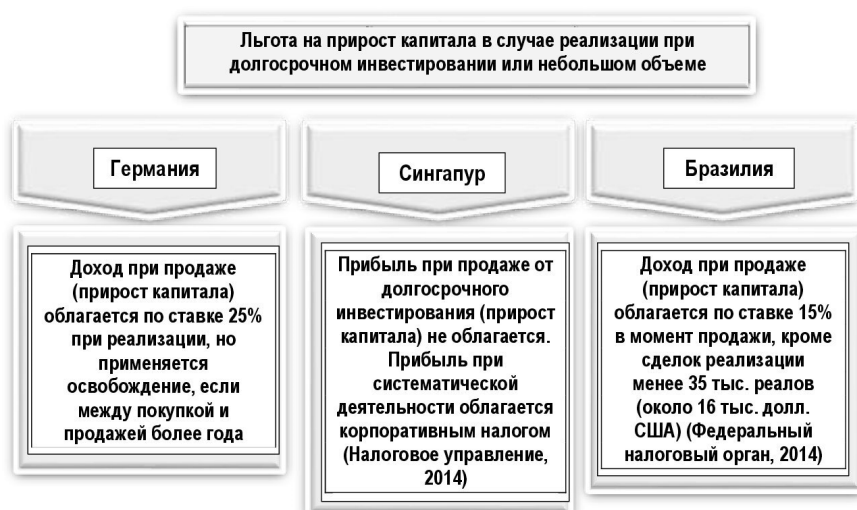


Рис. 5. Льготы на прирост капитала

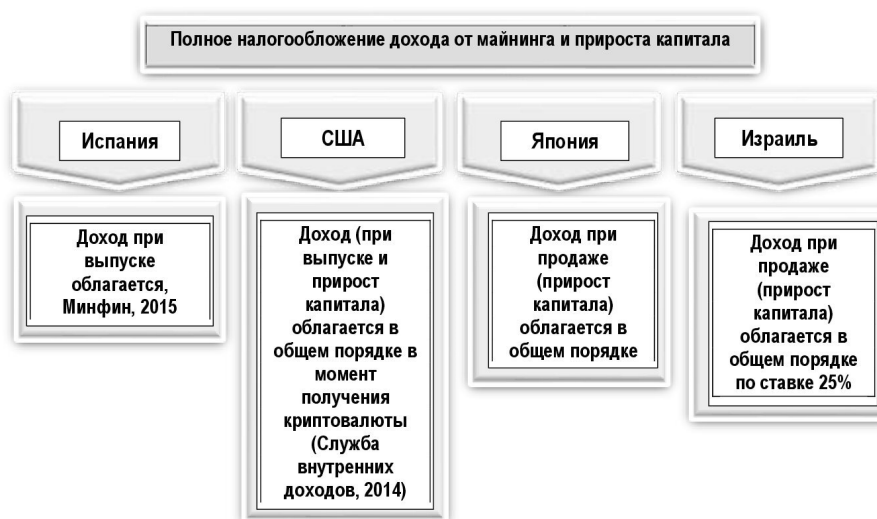


Рис. 6. Полное налогообложение



Рис. 7. Отсутствует нормативное правовое регулирование

Считаем, что целесообразно осуществлять государственное регулирование обращения цифровых валют по следующим направлениям [1]:

1. Цифровые валюты как средство платежа. Национальные регуляторы, прежде всего должны установить порядок определения стоимости данных валют, прогнозировать пределы их волатильности.

2. Цифровые валюты как надежные инвестиционные продукты. Определить порядок движения цифровых активов для инвесторов (покупка-продажа) их использования в виде биржевых индексных облигаций и деривативов с учетом предполагаемых рисков.

3. Законодательно регулировать деятельность криптобирж. Основная цель – недопущение отмывание незаконно полученных средств, а также противодействие финансированию террористической деятельности.

4. Определение стейблкоинов, путем введения «разумного» банковского контроля (пруденциальных требований). С этой целью стейблкоины «привязать» к курсам среднерисковым ценным бумагам и драгоценным металлам.

Для решения данных задач нужны дополнительные меры, представленные на рис. 8.

Потеря доходов бюджета от операций с цифровыми активами вызывает все более сильное беспокойство за устойчивость фискальной системы страны. Современные реалии показывают, что в условиях «санкционной войны» спрос на криптовалюту стремительно растет, не смотря на риски, волатильность и «мыльные пузыри» на данном рынке.

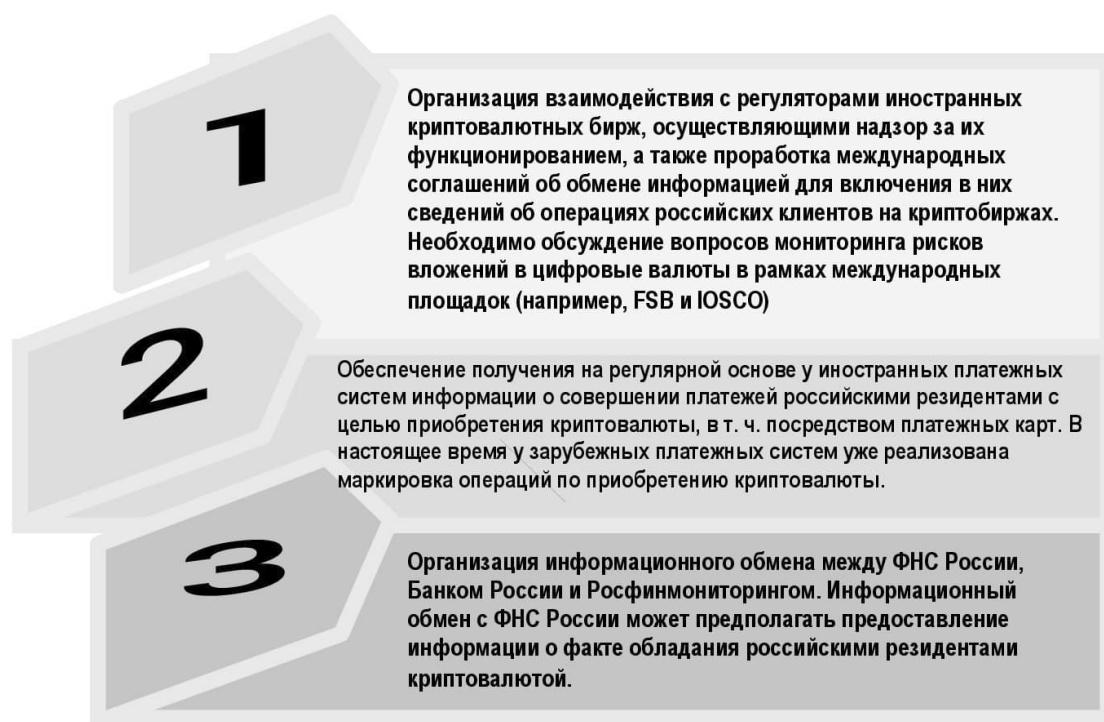


Рис. 8. Система мониторинга цифровых валют

Из-за межнационального характера цифровых валют и различий в нормативном регулировании цифровых активов возникает риск неэффективности регуляторного арбитража, так как есть большая вероятность «перетока» сделок (операций) под юрисдикции с «мягкими» регуляторными режимами.

Список литературы

1. Банк России. Криптовалюты: тренды, риски, меры. URL: <http://www.consultant.ru/law/hotdocs/73121.html/> (дата обращения: 21.07.2022).
2. Банки сегодня. Информационно-аналитическое финансовое издание. URL: <https://bankstoday.net/last-articles/zapretyat-li-v-rossii-kriptovalyuty-ekspertytsenivayut-initsiativy-vlastej/> (дата обращения: 21.07.2022).
3. Криптовалюта: пробелы регулирования. URL: <https://www.advgazeta.ru/mneniya/kriptovalyuta-probely-regulirovaniya/> (дата обращения: 21.07.2022).
4. Майнинг криптовалюты. Информационно-аналитический портал. Исследование: криптовалютные инвестиции в России и мире, реальность и перспективы. URL: <https://mining-cryptocurrency.ru/issledovanie-kriptovalyutnye-investicii-v-rossii-i-mire/> (дата обращения: 21.07.2022).
5. Пинская М. Р. Налогообложение доходов от деятельности, связанной с криптовалютами. URL: <https://cyberleninka.ru/article/n/nalogooblozhenie-dohodov-ot-deyatelnosti-svyazannoy-s-kriptovalyutami/> (дата обращения: 21.07.2022).
6. Отчет Центробанка по криптовалютам – выжимка с основными тезисами. URL: <https://habr.com/ru/post/646955/> (дата обращения: 21.07.2022).

С. К. Соломин,
доктор юридических наук, доцент,
профессор кафедры гражданско-правовых наук,
Кузбасский институт Федеральной службы исполнения наказаний
Российской Федерации,
заведующий кафедрой гражданского права,
Томский государственный университет систем
управления и радиоэлектроники

К ВОПРОСУ О ПРАВОВОЙ КВАЛИФИКАЦИИ КЕШБЭКА ПО БАНКОВСКОЙ КАРТЕ

Аннотация. В статье решается одна из насущных проблем современной цивилистической науки – определение правовой природы кешбэка по банковским картам. Отталкиваясь от положений экономической теории о кешбэке, автор рассматривает действия по возврату денежных средств на счет клиента исключительно через призму договора банковского счета и квалифицирует их в качестве возмещения на счет клиента излишне уплаченной суммы денег.

Ключевые слова: кешбэк, договор банковского счета, договор, на выдачу и использование банковской карты, банковская карта, расчетная операция, банк

TO THE QUESTION OF LEGAL QUALIFICATION OF CASHBACK ON BANK CARD

Abstract. The article solves one of the pressing problems of modern civilistic science – the definition of the legal nature of cashback by bank cards. Proceeding from the provisions of the economic theory of cashback, the author considers actions to return funds to the client's account exclusively through the prism of the bank account agreement and qualifies them as a refund to the client's account of an unnecessarily paid amount of money.

Keywords: Cashback, Bank account agreement, Agreement for issuing and using a bank card, Bank card, Settlement operation, Bank

Термин «кешбэк» (от англ. cashback) получил довольно широкое применение в различных сферах человеческой деятельности, начиная от деятельности профессиональных участников хозяйственного оборота и заканчивая социальной поддержкой населения. Общепринятое восприятие кешбэка как действия по возврату денежных средств отражает экономическую суть данного понятия, однако не позволяет дать точную правовую оценку тем явлениям и процессам реальной действительности, которые обозначаются этим термином. Так, например, туристический кешбэк и возврат части стоимости покупки в магазине через кешбэк-сервисы, обладая единой экономической сущностью, опосредуются различными друг от друга правовыми конструкциями, а соответственно, обладают разной правовой природой. Если суть туристического кешбэка сводится к субсидированию государством туристических поездок граждан в определенных на-

правлениях в пределах выделенных сумм, то кешбэк при покупке товаров через кешбэк-сервис представляет собой не более чем скидку на товар. Наибольшие затруднения возникают при правовой квалификации кешбэка по банковским (кредитным, дебетовым) картам, что в первую очередь связано с трудностями, возникающими при уяснении цели банковской операции по возврату денежных средств на счета клиентов. Для решения данного вопроса необходимо осознать некоторые экономические аспекты движения денег при предоставлении кешбэка как одного из видов банковского продукта.

Появившийся в конце 80-х гг. прошлого столетия в практике зарубежных банков (и прежде всего банков США) кешбэк по банковским картам было принято рассматривать через призму условий программы лояльности, стимулирующей клиента осуществлять покупки посредством пластиковой карты. В то время размер кешбэка составлял около 5 %, который уже к середине 90-х гг. (по мере достижения той цели, которую был призван выполнять кешбэк, а именно популяризации безналичных расчетов посредством применения банковских карт) снизился до 1 %. На отечественном рынке финансовых услуг кешбэк как банковский продукт стал предлагаться значительно позже (примерно с 2006 г.). Несмотря на то, что российские банки полностью заимствовали практику зарубежных банков, в том числе предоставление услуги кешбэка в рамках условий программы лояльности того или иного банка, возврат денежных средств на банковскую карту плательщика уже никто не связывал с выполнением стимулирующей функции – отказа от наличных расчетов в пользу безналичных.

В условиях российской действительности, когда вся работоспособная часть населения уже имела на руках как минимум одну пластиковую карту, данный банковский продукт использовался (и используется сейчас) лишь с одной целью – расширением клиентской базы конкретного коммерческого банка. Обозначенная цель предопределила качественный состав участников, предлагающих финансовую услугу по возврату денежных средств на счет владельца банковской карты. Речь идет прежде всего о частных коммерческих банках. По этой причине мы не найдем, например, в практике Сбербанка России, услугами которого пользуется большая часть населения нашей страны, хоть какое-то упоминание о кешбэке в чистом виде (т. е. в формате возврата денежных средств, а не баллов, которые начисляются по условиям программы лояльности «Спасибо»).

Последние пять лет частные коммерческие банки проводят весьма агрессивную политику по продвижению данного банковского продукта (взять, к примеру, коммерческий банк «Тинькофф»), но не за горами то время, когда он исчезнет. Некоторые специалисты, работающие на рынке финансовых услуг, еще несколько лет назад отмечали, что европейские банки в самое ближайшее время, скорее всего, откажутся от предоставления данного банковского продукта, что в первую очередь связано с источником возмещения денежных средств на счета клиентов – так называемой эквайринговой комиссией (комиссией за розничные расчеты по платежным картам в магазинах), часть которой банк-эквайер (банк, который предоставил платежный терминал) отдает банку-эмитенту (банку, выпустившему карту для расчетов). Именно за счет этой части комиссионных

банк-эмитент способен возмещать денежные средства на счета клиентов. Однако если в практике зарубежных банков этот размер комиссии постепенно стремится к нулю (что и предвещает исчезновение cashback из перечня банковских продуктов), то в нашей стране банки-эквайеры платят банку-эмитенту в пределах 1,5 %, что и позволяет последнему возмещать некоторые суммы на счета своих клиентов-плательщиков [1]. Однако, по мнению аналитиков, и российские банки в самое ближайшее время могут пересмотреть условия программ лояльности вплоть до их отмены [5].

Учитывая изложенное, нетрудно понять, что возмещение денежных средств на счета клиентов осуществляется за счет собственных средств банка. Вместе с тем правовая квалификация кешбэка применительно к указанному виду профессиональной деятельности не может быть сведена ни к средству стимулирования использования пластиковой карты при осуществлении расчетов, ни к средству привлечения клиентов в банк. Квалифицирующее значение при определении существа кешбэка по банковским картам приобретает лишь то, что отношения банка с его клиентами всегда имеют договорную природу, а значит, любое действие по возврату денежных средств на счет клиента осуществляется в рамках динамики заключенного договора.

Как правило, условие о кешбэке содержится в программе лояльности того или иного банка, к которой клиент банка присоединяется одновременно с заключением какого-либо договора, связанного с выдачей банковской карты. Это может быть, в частности, как непосредственно договор на выдачу, использование и обслуживание банковской карты, так и, например, ставший в последнее время популярным договор на комплексное банковское обслуживание физических лиц. Вместе с тем это никак не отражается на правовой природе условия о кешбэке: содержится ли такое условие в самом договоре или его приложении, оно всегда остается договорным, а значит, рассматривается в контексте содержания соответствующего договора. При этом важно уяснить один важный момент: содержание договора не может быть сведено лишь к одному условию о кешбэке, т. е. действие по возврату денежных средств на счет клиента не может составлять единственный (а равно основной) предмет договора. Объяснение этому тезису кроится в условиях применения кешбэка (в условиях возникновения обязанности возврата денег).

Обязанность банка вернуть деньги на счет клиента возникает только в том случае, если банком проведена какая-либо расчетная операция за счет средств, находящихся на счете клиента, с использованием банковской карты. То есть кешбэк (как расчетная операция) всегда выступает следствием совершения другой (основной) расчетной операции, а значит, и размер кешбэка всегда привязан к «стоимости» этой основной расчетной операции. Таким образом, проведение банком основной расчетной операции выступает тем необходимым условием, которое определяет момент возникновения его обязанности вернуть определенную часть произведенного платежа на счет клиента. Естественно, что, помимо обозначенного условия применения кешбэка, имеют место и другие. Но в отличие от проведения основной расчетной операции все остальные

условия не связаны с перемещением материального блага (движением денег по счетам), а выполняют организационную функцию (например, выбор категорий товара, по которым будет начисляться кешбэк, отсутствие просрочки по обязательствам перед банком и др.).

Любая расчетная операция за счет средств, находящихся на счете клиента, производится во исполнение его распоряжений. Банковская карта, выступая электронным средством платежа, определяет способ реализации одной из форм безналичных расчетов, а именно прямого дебетования (расчетов в форме перевода электронных денежных средств). Сама по себе банковская карта как предмет материального мира (кусочек пластика) не представляет никакой ценности. Все действия банка по выпуску банковской карты совершаются в рамках оказания соответствующей деятельности – оказания услуг банка, составляющих предмет договора банковского счета. И в этом смысле неважно, заключен ли договор банковского счета в виде отдельного договора-документа либо он входит в содержание комплексного договора (договора-документа), когда, например, по содержанию кредитного договора мы наблюдаем все атрибуты договора банковского счета, в частности условия об открытии счета и его обслуживании, в том числе касающиеся зачисления суммы кредита на открытый счет клиента. Поэтому, какое бы название ни имел договор, предполагающий выдачу банковской (дебетовой или кредитной) карты и ее обслуживание, он всегда будет оставаться договором банковского счета. В этой связи трудно согласиться с мнением Л. Г. Ефимовой о том, что договор о выдаче и использовании банковской карты относится к числу непоименованных договоров [3].

При определении правовой природы данного договора Л. Г. Ефимова отталкивалась от предложенной ею системы договоров об организации безналичных расчетов, в которую и включила договор о выдаче и использовании банковской карты. Последнее позволило ей заключить, что обозначенный договор является самостоятельным гражданско-правовым договором, построенным по модели рамочного договора [2. С. 117]. Вместе с тем данное умозаключение, на наш взгляд, вступает в противоречие с ее авторским определением данного договора. Правовед рассматривает договор о выдаче и использовании банковской карты исключительно через призму исполнения банком-эмитентом распоряжений держателя карты о совершении расчетных и кассовых операций. В качестве специфической особенности этого договора Л. Г. Ефимова называет документы, составленные с помощью электронных средств платежа (платежных терминалов, банкоматов, банковской платежной карты и т. п.) и направленные банку-эмитенту дистанционно по специальным каналам связи, которые в итоге и выступают условием исполнения распоряжений клиента.

Из определения видно, что этот договор порождает обязательственное правоотношение, объектом которого выступает оказание услуг со стороны банка-эмитента, а значит, априори не может выступать примером рамочного договора. Договор, построенный по модели рамочного договора, определяет лишь общие условия обязательственных взаимоотношений сторон (п. 1 ст. 429.1 ГК РФ), а значит, и возникшие из договора правоотношения являются не обязательственными,

а организационными: «Конструкция рамочного договора выступает отражением одного из специфических признаков определенной группы организационных договоров, а именно возможности развития взаимоотношений сторон этих договоров посредством установления новой обязательственной связи» [4. С. 126]. Как представляется, это понимает и сама Л. Г. Ефимова, когда сравнивает договор о выдаче и использовании банковской карты с договором банковского счета, выделяя одно отличие: «Договор о выдаче и использовании банковской карты предназначен для осуществления безналичных расчетов с помощью соответствующих технических устройств, которые делают возможным упрощенный порядок оформления расчетных документов» [3]. Данное «отличие» сводится исключительно к определению способа осуществления безналичных расчетов и не более. Замечу, что способ совершения действий не может восприниматься в качестве отличительного признака договорных типов (а равно видов договора в рамках одного договорного типа). Так, например, правила о договоре розничной купли-продажи предусматривают различные способы его исполнения, в том числе продажу товаров дистанционным способом и продажу товаров с использованием автоматов. Очевидно, что наличие технических устройств в подобных случаях выбора способа исполнения договора, когда отсутствует непосредственный контакт продавца и покупателя, не делает из этих договоров самостоятельные виды и тем более не позволяет относить их к числу рамочных договоров.

Таким образом, можно говорить о том, что исполнение обязанности банка возвратить денежные средства на счет клиента при использовании последней банковской карты происходит исключительно в рамках динамики договора банковского счета, а соответственно, сама обязанность возврата денежных средств подлежит восприятию в качестве одного из обязываний, составляющих содержание единой обязанности банка, оказание услуг, связанных с проведением операций по счету, открытому клиенту. Определив место кешбэку в цепочке действий, совершаемых банком, нетрудно раскрыть назначение кешбэка как расчетной операции: банк возмещает на счет клиента излишне уплаченную сумму денег, размер которой может быть рассчитан исключительно на стадии совершения основной расчетной операции.

Подобный подход к определению существа кешбэка позволяет, прежде всего, дать оценку банкам-эмитентам с точки зрения соблюдения ими требования добросовестности при разработке условий договоров банковского счета, к которым потенциальные клиенты присоединяются по правилам о договоре присоединения. В частности, каким бы привлекательным ни казалось условие о кешбэке, предлагаемое тем или иным банком, в динамике развития договорных правоотношений сумма возвращенных денежных средств всегда будет меньше суммы тех денежных средств, которые будут выплачены банку за выпуск и обслуживание банковской карты. Кроме того, стандартные условия договоров банковского счета (договора на выдачу и использование банковской карты) всегда содержат огромное число оговорок (условий возврата денежных средств на счет клиента), которые максимально сокращают число случаев

применения кешбэка. И это притом, что банк возмещает денежные средства, хотя и за счет собственных источников, но сформированных за счет денежных средств клиентов, перечисленных ранее не только в рамках основной расчетной операции (т. е. операции, по которой рассчитывается процент кешбэка), но и по всем остальным расчетным операциям, не попавшим под действие условий программы лояльности.

Список литературы

1. Cash-back: выгодно отдать деньги. URL: <https://ksonline.ru/282616/sash-back-vygodno-otdat-dengi/> (дата обращения: 17.07.2022).
2. Ефимова Л. Понятие, правовая природа и предмет договора о выдаче и использовании банковской карты // Хозяйство и право. 2015. № 11 (466). С. 117–128.
3. Рождественская Т. Э., Гузнов А. Г., Ефимова Л. Г. Частное банковское право: учебник. Москва: Проспект, 2020. 776 с.
4. Соломин С. К., Соломина Н. Г. Систематизация гражданско-правовых договоров: монография. Москва: Юстицинформ, 2021. 152 с.
5. Эксперты оценили влияние эквайринговой комиссии на размер кэшбэка. URL: <https://www.banki.ru/news/lenta/?id=10963352> (дата обращения: 20.07.2022).

С. В. Соляник,

магистр сельскохозяйственных наук,
Национальная академия наук Беларуси
по животноводству

В. В. Соляник,

кандидат сельскохозяйственных наук, доцент,
Национальная академия наук Беларуси
по животноводству

ЦИФРОВИЗАЦИЯ ЗООТЕХНИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ КАК МЕХАНИЗМ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЖИВОТНОВОДСТВА НОРМАМИ АГРАРНОГО ПРАВА

Аннотация. Цифровизация производства продукции животного происхождения, а также зоотехнической науки, как научной основы этого вида экономической деятельности, позволяет в режиме реального времени проводить имитационное моделирование риск-сценариев работы любого животноводческого объекта (фермы, комплекса, фабрики и др.). При это только цифровизация дает возможность установить те правовые механизмы, в данном случае в области аграрного права, которые необходимы и достаточны для повышения эффективности, в том числе финансовой, предприятий в сфере производства продукции животного происхождения. Учеными в области зоотехнии и зоогигиены, которые разработали цифровые двойники для ведения животноводства, обоснованы четыре законопроекта: «О зоотехнии и зоотехнической деятельности», «О породах животных

и генофондных хозяйствах», «Об обеспечении деятельности сельскохозяйственных организаций», «О гармонизации объемов экспорта мясо-молочной продукции и научно обоснованном стимулировании импортозамещения сельскохозяйственного сырья и продовольствия».

Ключевые слова: аграрное право, зоотехния, зоогигиена, производство продукции животного происхождения, цифровизация

DIGITALIZATION OF ZOOTECHNICAL ACTIVITIES AS A MECHANISM OF LEGAL REGULATION OF ANIMAL HUSBANDRY BY NORMS OF AGRARIAN LAW

Abstract. The digitalization of the production of products of animal origin, as well as zootechnical science, as the basis of a type of economic activity, makes it possible to simulate risk scenarios for the operation of any livestock facility (farms, complexes, factories, etc.) in real time. At the same time, only digitalization makes it possible to establish those legal mechanisms, if they are applied in the field of agricultural law, that are necessary and sufficient to increase efficiency, including for financial activities in the production of products of animal origin. Scientists in the field of zootechnics and zoohygiene, who developed digital twins for animal husbandry, founded four bills: “On zootechnics and zootechnical activities”, “On animal breeds and farm gene pools”, “On the harmonization of export volumes of meat and dairy products and scientifically based stimulation of import substitution of agricultural raw materials and food”.

Keywords: Agrarian law, Zootechnics, Zoohygiene, Production of products of natural origin, Digitalization

Введение. В практической деятельности зоотехники-селекционеры сельскохозяйственных организаций нашей страны руководствуются прежде всего теми знаниями и компетенциями, которые они приобрели в стенах средних специальных и высших учебных заведений. В то же время, специалисты в области животноводства порой даже не знают о наличии законодательства о племенном деле в животноводстве, которое является источников аграрного права.

Источники аграрного права – внешняя форма выражения государственной воли, закрепления аграрно-правовых норм, применяемых для регулирования аграрных отношений. Под нормой права понимается общее (неперсонифицированное) правило поведения, обязательное для исполнения гражданами и должностными лицами, установленное уполномоченным на то государственным органом с соблюдением установленной законодательством процедуры [1. С. 21].

Согласно ст. 3 Закона Республики Беларусь «О племенном деле в животноводстве» от 20.05.2013 № 24-3 [2] государственное регулирование и управление в области племенного дела осуществляются Президентом, Советом Министров, Министерством сельского хозяйства и продовольствия, местными Советами депутатов, исполнительными и распорядительными органами в пределах их компетенции, а в ст. 4–7 Закона определены их полномочия.

В Государственной программе развития аграрного бизнеса в Республике Беларусь на 2016–2020 гг. перечисляются 15 мероприятий по племенному делу

в животноводстве [3], которые начинаются со слов проведение; удешевление; сохранение; выращивание, реализация и закупка; подготовка и проведение; формирование; переоснащение; разработка, развитие (совершенствование), внедрение и реализация; издание; вступление. По сути, этими словами описываются длящиеся, ни к чему не обязывающие процессы. Дело в том, что мероприятия подпрограммы – это структура фактического распределения денежных средств, выделяемых ежегодно из республиканского бюджета на их выполнение.

В чуть более десяти технических нормативных правовых актов, составляющих наряду с Законом, законодательство о племенном деле в животноводстве, изложена специальная зоотехническая информация по объему превышает 393 тыс. печатных знаков, а с учетом самого закона – более 420 тыс. знаков. По сути, эта информация соотносится с объемом «стандартной» монографии в 10 авторских листов.

Как нестранно, но о содержании закона и подзаконных актов зоотехники-ученые и зоотехники-практики не имеют четкого представления. Дело в том, что в разработке законодательных основ ведения племенного животноводства принимали участие представители (преимущественно руководители) органов государственного управления, т. е. Минсельхозпрода, Национальной академии наук Беларуси. Основную роль при формировании норм и правил играли юристы этих госорганов, а также специалисты Национального центра законодательства и правовых исследований Республики Беларусь.

В итоге нормативно-правовая база в области племенного дела представляет собой заформализованное перечисление понятий и терминов, о которых студенты зоотехнических факультетов вузов и отделений колледжей знают из специальной образовательной дисциплины «Разведение сельскохозяйственных животных», включающий курс «Племенное дело», по объему не превышающим 1 % от всей дисциплины.

В принятом законодателем законе имеется существенный пробел, так как отсутствует дефиниция термина «бонитировка», а разработчики технического нормативного правового акта декларативно указывают о экспертах-бонитерах и даже о целой службе независимых бонитеров, о которых уже четверть века в Беларуси никто не слышал.

Белорусское законодательство о племенном деле в животноводстве, как и его правоприменение имеют правовые пробелы и коллизии, не позволяющие на надлежащем уровне вести племенную работу в нашей стране. Основная проблема технического нормирования в области племенного дела в животноводстве заключается в том, что все нормативные предписания технических правовых актов должны исполнять специалисты, имеющие среднее специальное или высшее образования в области зоотехнии, но в законодательстве о племенном деле в животноводстве ничего не сказано ни о зоотехнии, ни о зоотехнической деятельности [4].

Основная часть. Согласно ст. 1 Закона Республики Беларусь «О племенном деле в животноводстве» от 20.05.2013 № 24-З [2]: племенное дело в животноводстве – комплекс зоотехнических, селекционных и организационно-хозяйственных мероприятий, направленных на создание, сохранение, улучшение полезных наследственных качеств племенных животных и их рациональное использование для получения (производства) продуктов животного происхождения.

Белорусский Законодатель не раскрывает значение выражения «комплекс зоотехнических, селекционных и организационно-хозяйственных мероприятий».

При этом, согласно пункта 16 ст. 3.30 Процессуально-исполнительного кодекса Республики Беларусь об административных правонарушениях [5] должностные лица Министерства сельского хозяйства и продовольствия, подчиненных ему государственных организаций, органов государственной ветеринарной и племенной служб, уполномочены составлять протоколы об административных правонарушениях по ст. 16.28 (Нарушение требований в области ветеринарной деятельности) Кодекса об административных правонарушениях Республики Беларусь [6]. Таким образом, нарушение в сфере зоотехнической деятельности, к которой относится племенное дело в животноводстве, согласно законодательству об административных правонарушениях, «регламентируется» законодательством о ветеринарной деятельности, что некорректно с точки зрения основ аграрного права.

Нами предлагаются следующие дефиниции в ст. 1 Закона Республики Беларусь «О племенном деле в животноводстве» от 20.05.2013 № 24-З [2]:

– Зоотехнические мероприятия – комплекс организационных и технологических процедур по разведению, кормлению, гигиене содержания и ухода за породами животных. Зоотехнические мероприятия регламентируются техническими нормативными правовыми актами.

– Селекционные мероприятия – племенная работа, основанная на классических методах и способах разведения животных, направленная на планомерное повышение продуктивных и качественных характеристик чистопородного поголовья животных и снижение себестоимости производства продукции животноводства.

Селекционные мероприятия, целью которых является создание новых пород животных (селекционные достижения), регулируются техническими нормативными правовыми актами.

Практической основой осуществления селекционных мероприятий является надлежащее ведение племенных книг. Племенные книги по каждой породе животных, разводимых в Республике Беларусь, размещаются в свободном доступе в глобальной сети Интернет в неизменном виде (в формате PDF). Переиздание племенных книг производится по мере необходимости, но не реже одного раза в пять лет.

Правовая охрана селекционных достижений регулируется нормами законодательства об интеллектуальной собственности.

– Организационно-хозяйственные мероприятия – это комплекс технологических процедур по надлежащему выполнению нормативных требований ведения племенной работы с породами животных в племенных и генофондных хозяйствах. Технологические процедуры регламентируются техническими нормативными правовыми актами.

Упоминание технических нормативных правовых актов в дефинициях зоотехнических, селекционных и организационно-хозяйственных мероприятий относится исключительно к действующему в Республике Беларусь законодательству о племенном деле в животноводстве.

На наш взгляд законодательство о племенном деле в животноводстве – это не столько необоснованное вмешательство государства в хозяйственную деятельность, сколько избыточное правовое регулирование в сфере животноводства.

Российский политолог, публицист и юрист, старший научный сотрудник Университетского колледжа Лондона В. Пастухов в лекции «Почему в России не работают законы» указывал, что: «Если вы спросите меня, что есть главное в праве, я вам отвечу: в праве главное – процедура. В праве главное – определенная способность к правовому логическому мышлению. Именно поэтому Берман, который успел еще почитать лекции, даже приехав в горбачевский СССР, и который является одним из ведущих философов права в XX в., написавшим книгу «Западная традиция права», полагал, что главное в праве – воспитание особой касты людей, обладающих профессиональным правовым сознанием. Воспитание этого профессионального правового сознания – очень сложная, специфическая вещь. Потому что – поверьте мне, я сам принадлежу к числу этих психически не совсем здоровых людей, которых мы называем юристами, – настоящий юрист (не то, что принято сегодня называть юристами в нашей замечательной стране) – это, к сожалению, всегда человек ущербный.

Потому что он смотрит на мир всегда через очень узкую щель нормативистского сознания. То есть он смотрит и оценивает любое явление только с точки зрения того, как оно может быть описано той или иной правовой нормой. И именно эта способность воспринимать мир через норму, интерпретировать все, что происходит вокруг, нормативистски, и есть суть профессионального правового сознания. И на наличии касты людей, которые смотрят на мир подобным образом, держится современная правовая система» [7].

Таким образом, профессиональное правосознание – это когда человек-профессионал рассматривает какую-либо сферу деятельности через формализацию конкретных норм права, способствующих успешному ее регулированию.

Нами, учеными-зоотехниками, имеющими высшее юридическое образование, предлагается лаконичная «конституция производителей продукции животного происхождения»:

Ст. 1. Физическим и юридическим лицам запрещено осуществлять уход за животными, если на текущий момент отсутствуют высококачественные корма в зоотехнически обоснованных объемах, или условия содержания особей зоологического вида не соответствуют зоогигиеническим нормам и правилам.

Ст. 2. Если по зоотехническим расчетам баланс кормов выполняется до определенной календарной даты, то необходимо заблаговременно провести технологические мероприятия по плановому сокращению поголовья животных до количества, позволяющего не допустить обстоятельств, указанных в ст. 1.

Это конституция основана на цифровизации зоотехнической науки и животноводства в целом. Национальный центр интеллектуальной собственности Республики Беларусь в нынешнем году выдал 11 Свидетельств о добровольной регистрации и депонировании объекта авторского права на компьютерные программы:

– Цифровой двойник технологических характеристик свиноматок, в зависимости от месяца их рождения, и хряков-производителей – от месяца начала полового использования;

– Цифровые двойники зоотехнического и химического состава кормов растительного происхождения;

- Цифровой двойник морфологических, биохимических, иммунологических характеристик крови свиней и уровня продуктивности молодняка свиней и свиноматок;
- Цифровой двойник гигиенических качественных характеристик свинины;
- Цифровой двойник имитационного моделирования оптимальных по питательности и минимальных по стоимости рационов кормления животных;
- Цифровой двойник теплофизических характеристик строительных материалов и ограждающих конструкций животноводческих зданий;
- Цифровой двойник тепло-, влаго-, газовыделений животных, уровня их кормления и продуктивности в зависимости от значений параметров микроклимата помещений;
- Цифровой двойник теплофизических процессов, с почасовой, суточной и сезонной динамикой, в зданиях для содержания животных различных зоологических видов, и комплексного аудита надлежащего выполнения зоогигиенических норм и правил;
- Цифровой двойник систем водораспределения, водопотребления, водоотведения, навозоудаления животноводческих зданий, процессов переработки навозных масс, получения качественных органических удобрений, повышения плодородия почв и аудита надлежащего выполнения требований биологической безопасности объектов;
- Цифровой двойник оценки воздействия на окружающую среду территорий размещения животноводческих объектов, скрининга концентрации загрязнения атмосферного воздуха в межкорпусных и циркуляционных зонах животноводческих зданий, аудита надлежащего выполнения экологических норм и правил;
- Цифровой двойник системы объективного контроля кадастровой оценки сельскохозяйственных земель и оптимального севооборота, анализа размера природной ренты, объема производства основной и побочной продукции растениеводства и животноводства, моделирования риск-сценариев и мониторинга финансовой эффективности функционирования сельскохозяйственного предприятия.

Таким образом цифровая зоотехния и животноводство, в настоящее время, основывается на 11 стратегических цифровых двойниках, включающих более 60 тактических цифровых двойников, которые в свою очередь насчитывают сотни оперативных цифровых двойников. В последующем мы планируем создать еще несколько стратегических цифровых двойников исключительно под различные зоологические виды.

Цифровизация зоотехнической науки и производственного процесса получения продукции животного происхождения должна базироваться на лаконичных (5–10 норм) нормативных правовых актах – законах прямого действия, чтобы отслеживать в режиме реального времени надлежащее исполнение субъектами аграрного права норм зоотехнического (агрофаунистического) права [8].

Нами разработаны следующие проекты законов: 1) «О зоотехнии и зоотехнической деятельности», 2) «О породах животных и генофондных хозяйствах», 3) «Об обеспечении деятельности сельскохозяйственных организаций», 4) «О гармонизации объемов экспорта мясо-молочной продукции и научно обоснованном стимулировании импортозамещения сельскохозяйственного сырья и продовольствия».

1. О проекте Закона Республики Беларусь «О зоотехнии и зоотехнической деятельности». В Республике Беларусь за обращения с животными «отвечают» почти все министерства и ведомства (включая силовые и правоохранительные), общественные организации, зооактивисты и зооволонтеры.

В то же время единственными специалистами в сфере обращения с животными (независимо от зоологического вида), которая включает профессиональное разведение, кормление, содержание и уход за конкретными половозрастными группами животных, являются граждане, имеющие среднее специальное или высшее образование в области «Зоотехния».

В связи с тем, что компетенциями и квалификацией обращения с животными обладают исключительно зоотехники-практики и ученые-зоотехники, необходимо разработать и принять Закон Республики Беларусь «О зоотехнии и зоотехнической деятельности».

С вступлением в действие Закона Республики Беларусь «О зоотехнии и зоотехнической деятельности» появится реальная возможность создать в стране единую прозрачную систему контроля и надзора за животными по обеспечению их благополучия, биологической безопасности и сохранения зоологического разнообразия.

2. О проекте Закона Республики Беларусь «О породах животных и генофондных хозяйствах». Во второй половине XIX в. чистокровные животные относились к конкретной породе, утвержденной ассоциацией заводчиков, которые приобретали статус племенных животных владельцем которых имел право реализации самцов-производителей и самок другим собственникам. для налаживания и ведения племенной работы с целью увеличения генетического потенциала стада и его продуктивности, а иногда и для выведения новой породы.

Спустя сто лет, во второй половине XX в. в большинстве государств на планете поголовье сельскохозяйственных животных относилось к той или иной породе, т. е. из местных малопродуктивных животных они превратились в чистопородный высокопродуктивный скот. При этом если на животных конкретного стада велась племенная книга, которая периодически издавалась и была доступна для животноводов, то поголовье скота этой породы относилось к племенным животным.

Согласно Приложения № 3 к постановлению ЦК КП Белоруссии и Совета Министров БССР (21.01.1959 № 76) был утвержден План размещения пород сельскохозяйственных животных, в котором были перечислены плановые породы животных по административным районам БССР:

- скотоводство: симментальская и местный симментализированный скот; черно-пестрые (остфризская и эстонская черно-пестрая); красные (красная эстонская и красный белорусский скот); бурые (бурая латвийская, швицкая и костромская);
- свиноводство: крупная белая; белорусская черно-пестрая (Сторобинский район); чаусская (Кобринский район, Чауский район); крупная черная (Мстиславский район); брейтовская (Шкловский район);
- овцы: прекос, романовская, латвийская темноголовая.

Таким образом, в середине прошлого века на территории нынешней Беларуси в общественном животноводстве было 17 (семнадцать!) пород: 9 пород в скотоводстве; 5 пород в свиноводстве и 3 породы овец. Однако, белорусские породы жи-

вотных своевременно не были надлежащим образом зарегистрированы (утверждены), как например костромская порода крупного рогатого скота., которая была официально признана приказом по Народному комиссариату земледелия СССР «О костромской породе крупного рогатого скота» (27.11.1944 № 1121).

В течении последних трех десятилетий при непосредственном руководстве Белплемообъединения Минсельхозпрода в страну, преимущественно за средства республиканского бюджета, импортированы десятки тысяч голов сельскохозяйственных животных зарубежной селекции, что повсеместно позволило осуществить поглотительное скрещивание местных пород скота. При действии в нашей стране законодательства о племенном деле в животноводстве никакой реальной племенной работы по сохранению генетического разнообразия аборигенных пород животных не велось и не ведется. Как итог, уже к концу 90-х гг. XX в. в Беларуси не осталось ни одной из пород сельскохозяйственных животных, которые были в середине прошлого века.

Для реализации Соглашения о мерах, направленных на унификацию проведения селекционно-племенной работы с сельскохозяйственными животными в рамках Евразийского экономического союза, от 25 октября 2019 г., разработанного в целях реализации подпункта 4 пункта 1 ст. 95 Договора о Евразийском экономическом союзе от 29 мая 2014 г., необходимо принять Закон Республики Беларусь «О породах животных и генофондных хозяйствах».

3. О проекте Закона Республики Беларусь «Об обеспечении деятельности сельскохозяйственных организаций». Для успешного осуществления деятельности сельскохозяйственных организаций государством принимаются различные нормативные правовые акты, в том числе выделяются значительные суммы денежных средств на возведение новых объектов в растениеводстве и животноводстве. Однако однозначно не решены вопросы по снижению себестоимости производства продукции растительного и животного происхождения и повышению финансовой доходности от этого вида экономической деятельности, исключение коррупционных проявлений в функционировании сельскохозяйственных организаций.

Чтобы раз и навсегда решить вопросы с приписками или с сокрытием информации о негативных тенденциях в белорусских сельхозорганизациях в целом (наличие и использование удобрений; ремонт техники; количество и качество заготовленных кормов; урожайность; удои-привесы; численность скота и др.), необходимо вывести за штат всех специалистов (главный, средних, помощников и пр.), которые непосредственно не заняты в работе с животными и растениями, оставив только животноводов, полеводов и механизаторов, а также руководителя и двух его заместителей.

Для реализации этой цели необходимо принять Закон Республики Беларусь «Об обеспечении деятельности сельскохозяйственных организаций».

4. О проекте Закона Республики Беларусь «О гармонизации объемов экспорта мясо-молочной продукции и научно обоснованном стимулировании импортозамещения сельскохозяйственного сырья и продовольствия». Мониторинг государственной статистической отчетности показал, что импортная составляющая в экспорте белорусской сельскохозяйственной продукции занимает более $\frac{3}{4}$. Например, в 2015 г. импорт составлял 101 %, в 2016 г. – 97 %, в 2017 г. –

92 %, в 2018 г. – 84 %, в 2019 г. – 80 %. Условно говоря экспортируя сельхозпродукции на 5 млрд долл. США, Беларусь ее импортирует на 4 млрд долл. США.

По общему правилу Глобальный индекс продовольственной безопасности рассчитывается по 59 показателям и четырем критериям (доступность продуктов питания; их наличие; качество и безопасность; разнообразие природных ресурсов и их устойчивость). Среди показателей немаловажное место занимают государственные расходы на сельскохозяйственные научные исследования и разработки, доступ к технологиям, образованию и ресурсам, инвестиции в помещения для улучшения хранения урожая и др.

Для агропромышленного комплекса нашей страны важно иметь прозрачный правовой механизм, обеспечивающий гармонизацию объемов экспорта-импорта мясомолочной продукции и стимулирование импортозамещения сельскохозяйственного сырья и продовольствия. Этот механизм даст возможность значительно сократить импортную составляющую в экспорте сельскохозяйственной продукции, увеличит реальный объем валютной выручки, и на порядок снизить вывоз валюты для оплаты импорта сельхозпродукции. В рамках реализации НПА появится возможность улучшить значение ряда показателей Глобального индекса продовольственной безопасности и подняться в международном рейтинге, а также будет отмечаться реальное увеличение государственного финансирования аграрной науки, образования и инноваций в нашей стране.

В связи с вышеизложенным необходимо принять Закон Республики Беларусь «О гармонизации объемов экспорта мясо-молочной продукции и научно обоснованном стимулировании импортозамещения сельскохозяйственного сырья и продовольствия».

Учитывая, что предлагаемые законопроекты будут прямого действия, то не понадобится разработка и принятие технических нормативных правовых актов для их исполнения. Правоприменительная практика законодательства в области племенного дела в животноводстве показала, что никто из зоотехников-практиков и зоотехников-ученых незнаком с содержанием ни Закона Республики Беларусь «О племенном деле в животноводстве», ни многочисленных технических нормативных актов, принятых для его исполнения. И это несмотря на то, что НПА о племенном деле в животноводстве относятся к законодательству о предпринимательской, хозяйственной (экономической) деятельности, где основной тезис не навреди.

«Если мы говорим о том, что право объективно, что оно существует как бы вне нашей воли, вне нашего воображения, мы можем только его вычислять, то мы должны сказать о том, что является главным свойством права. Потому что у права, как и у любого явления, десятки свойств. Но мы должны выбрать какое-то главное из них, потому что от этого зависит дальнейшая приоритизация практическая всего того, что мы делаем. И в этом смысле главным и сущностным свойством права является его формальность. То есть право существует постольку и настолько, постольку оно формально.

Право – это всегда определенная процедура, это всегда определенная механика, это всегда набор каких-то ритуалов. Почему это так важно? Потому что иначе мы не можем сцедить эту объективность в субъективном. Особенность права, как и любой человеческой деятельности, в том, что оно как бы существует внутри нашей деятельности. Наша деятельность субъективна, потому что реализацией правового

занимаются десятки и сотни миллионов людей, каждый из них действует по своему усмотрению, со страстью, умыслом и так далее. И при этом из всей многообразной субъективной деятельности каким-то образом нужно отжать ту самую объективность права, те самые математические пропорции справедливости, которые не зависят ни от какого субъективного фактора. По сути, это такая машина для дистилляции, некий гигантский правовой механизм, который на входе получает кучу субъективного, а на выходе он должен получить совершенно объективный результат» [7].

Заключение. Прежде чем принимать нормативные правовые акты, в том числе и законы, в области предпринимательской, хозяйственной (экономической) деятельности необходимо, чтобы профессионалы в этих сферах провели их оцифровку, т. е. создали цифровые двойники.

Цифровизация производства продукции животного происхождения, а также зоотехнической науки, как научной основы этого вида экономической деятельности, позволяет в режиме реального времени проводить имитационное моделирование риск-сценариев работы любого животноводческого объекта (фермы, комплекса фабрики и др.). При этом только цифровизация дает возможность установить те правовые механизмы, в данном случае в области аграрного права, которые необходимы и достаточны для повышения эффективности, в том числе финансовой, предприятий в сфере производства продукции животного происхождения.

Учеными в области зоотехнии и зоогигиены, которые разработали цифровые двойники для ведения животноводства, обоснованы четыре законопроекта: «О зоотехнии и зоотехнической деятельности», «О породах животных и генофондных хозяйствах», «Об обеспечении деятельности сельскохозяйственных организаций», «О гармонизации объемов экспорта мясо-молочной продукции и научно обоснованном стимулировании импортозамещения сельскохозяйственного сырья и продовольствия».

Список литературы

1. Воронько Е. В. Аграрное право: электронный учебно-методический комплекс для студентов специальности 1–24 01 02 «Правоведение» // Научно-технический совет УО «Минский инновационный университет» (протокол № 5 от 27.04.2017). Рег. № ЭУМК 11-АП-38. – Минск, 2017. – 318 с.
2. О племенном деле в животноводстве: Закон Республики Беларусь от 20.05.2013 № 24-З // Национальный правовой интернет-портал Республики Беларусь, 22.05.2013, 2/2022.
3. Мероприятия подпрограммы 4 «Развитие племенного дела в животноводстве»: Приложение 8 к Государственной программе развития аграрного бизнеса в Республике Беларусь на 2016–2020 годы // Национальный реестр правовых актов Республики Беларусь 23.03.2016 № 5/41842.
4. Соляник С. В., Соляник В. В. Технические нормативные правовые акты как источники права надлежащего исполнения закона Республики Беларусь «О племенном деле в животноводстве» // Модернизация аграрного образования: Сб. науч. тр. по материалам VII Международ. науч.-практ. конф. (14 декабря 2021 г.) – Томск-Новосибирск: ИЦ Золотой колос, 2021. С. 564–573.
5. Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях от 06.01.2021 № 92-З / Национальный правовой интернет-портал Республики Беларусь, 22.01.2021, 2/2812.

6. Кодекс Республики Беларусь об административных правонарушениях 06.01.2021 № 91-3 / Национальный правовой интернет-портал Республики Беларусь, 22.01.2021, 2/2811.

7. Пастухов В. «Реконструкция права. Как восстановить то, чего не было». URL: <https://m.polit.ru/article/2022/03/06/archive2/> (дата обращения: 6 марта 2022 г.).

8. Чернов А. В. Рецензия на монографию «Особенности и проблемы правового регулирования животноводства» А. В. Соляника, В. В. Соляника // Вестник Белорусской государственной сельскохозяйственной академии. 2011. № 4. С. 196–198.

В. В. Сомонов,

заместитель директора,

Центр развития института интеллектуальной собственности,
аспирант факультета технологического менеджмента и инноваций,
Национальный исследовательский университет ИТМО

А. С. Николаев,

кандидат экономических наук, доцент, директор,

Центр развития института интеллектуальной собственности,
Национальный исследовательский университет ИТМО

ИСПОЛЬЗОВАНИЕ ПАТЕНТНОЙ АНАЛИТИКИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИННОВАЦИОННЫХ ПРОЕКТОВ

Аннотация. В статье определяется важность применения инструментов патентной аналитики в составе инструментов обеспечения информационной безопасности инновационных проектов, продемонстрированы показатели, на основе которых могут быть приняты управленческие решения по эффективному развитию и внедрению на рынок новых разработок. Выводы и рекомендации авторов основываются на анализе патентной активности на рынке цифровых технологий. В работе показано, что анализ патентной информации, позволяет качественно выполнить сегментацию рынка, выявить текущее положение конкурентов в занимаемых технологических сферах, включая их патентные стратегии на рынке и оценить перспективные направления развития технологий. Результаты патентных исследований имеют важное значение в рамках реализации мер поддержки промышленного развития отдельных регионов страны.

Ключевые слова: патентная аналитика, цифровые технологии, динамика патентования, технологические кластеры, ведущие правообладатели, срок жизни патентов

THE INFLUENCE OF PATENT ANALYTICS ON THE INFORMATION SECURITY OF INNOVATIVE PROJECTS

Abstract. The article shows the influence of patent analytics on the information security of innovative projects. It is indicated that management decisions can be made on the effective development and introduction of new developments to the market based on the demonstrated indicators. One of the rapidly developing areas of digital technologies, additive

manufacturing (selective laser melting) was analyzed as an example. The study showed that the analysis of patent information allows performing market segmentation, identifying the current position of competitors in the occupied technological areas, including their patent strategies in the market and evaluating promising areas of technology development.

Keywords: Patent analytics, Digital technologies, Patenting dynamics, technology clusters, Leading copyright holders, Patent lifetime

Введение. Обеспечение технологического суверенитета является одной из ключевых задач развития российской науки и промышленности. Лидерские позиции на мировой арене способны занимать государства, обладающие собственными развитыми технологиями и сильным кадровым потенциалом [8]. Все это вынуждает крупных игроков рынка постоянно совершенствоваться и разрабатывать новые технические решения в различных областях науки, особенно в цифровых технологиях, которые после внедрения смогут стать инновациями. В современном мире для эффективного управления проектами, связанными с инновационными разработками, особенно в сфере цифровых технологий необходимо раннее выявление технических решений, обладающих высоким потенциалом коммерциализации [6]. Разработки, основанные на недостаточном понимании потребностей рынка, редко оказываются прорывными [7]. Все чаще руководителям, чтобы принимать более обоснованные решения приходится использовать результаты анализа больших массивов данных.

Основная роль аналитических инструментов заключается в сборе информации из различных источников и преобразовании ее в полезную информацию для дальнейшего анализа. Бизнес-лидеры могут использовать эту информацию и сочетать ее со своим личным опытом для принятия окончательных решений. Организация часто сталкивается с проблемами низкого уровня грамотности сотрудников ее исследовательских подразделений в области интеллектуальной собственности и пренебрежительное отношение к результатам интеллектуальной деятельности, приводящими к преждевременному раскрытию ценной потенциально коммерчески привлекательной информации, полученной в результате исследований, до момента своевременного придания ей оптимальной формы правовой охраны. Все это подрывает информационную безопасность инновационных разработок, осуществляемых в компании и снижает ее конкурентные преимущества на рынке. Понимание реальной ценности и значимости собственных технологий позволяет обеспечивать рациональное управление в условиях быстро изменяющихся экономических реалий.

Для совершенствования механизма принятия управленческих решений, связанных с инновационным развитием и предотвращения информационных утечек в компаниях должна быть выстроена система поддержки выявления и опережающего патентования результатов интеллектуальной деятельности, связанных с разработками в сфере цифровых технологий. На этапе планирования инновационной разработки необходимо из множества вариантов, заложенных в проекте, выбрать тот, который значительно увеличит показатели конкурентоспособности, позволит захватить и сохранить лидерство в течение длительного периода времени [5]. Исследователи отмечают, что существует взаимосвязь между количеством запатентованных результатов интеллектуальной деятельности (далее – РИД) и доходом от их вовлечения в экономический оборот [13]. Патентный анализ широко используется в исследованиях

инноваций для оценки и мониторинга технологических изменений в различных секторах экономики [2]. Патенты являются обширным источником технических и коммерческих знаний, значимым опережающим индикатором того, куда направляются усилия компании в области НИОКР и инноваций. Рост числа патентных заявок по всему миру из-за расширения деятельности в области НИОКР подстегнул спрос компаний на аналитические решения [12]. Отдельный патент может быть лишь наброском потенциального продукта, но в совокупности патентная деятельность может выявить стратегическое направление и приоритеты компании [4]. В погоне за продвижением инновационного проекта компания может пропустить этап проведения надлежащего патентного поиска и при этом потратить много денег на разработку продукта, проведение испытаний, маркетинг, брендинг, поиск каналов распространения и многие другие дорогостоящие процессы чтобы потом обнаружить, что продукт уже был описан в более ранней патентной публикации, или, что еще хуже, защищен патентом, принадлежащим конкурирующей фирмой. Эффективно проведенный анализ патентной документации позволяет предприятию избежать ошибок в области выбора той, технологии на которую оно будет ставку, предсказать влияние того или иного патента на развитие предприятия, оценить возможности ближайших конкурентов, а за счет извлечения технической информации получить конкурентное преимущество в выбранной области технологий [1]. Часто патентную аналитику воспринимают как общий анализ патентной документации, не дающий конкретных рекомендаций, а выявляющий лишь тенденции в патентовании, не позволяющий узко специализировавшимся компаниям применять эти результаты в своей деятельности.

Применяя патентную аналитику компании способны на раннем этапе выявить угрозы для своей позиции на рынке [11] в связи с появлением перспективных изобретений или компаний, совершивших технологический прорыв, факт патентования бывшим сотрудником наработок компании в другой организации, наличие перекрывающих патентов на технологии и оборудование, используемое в производственном процессе компании на территории конкретных стран, избежать возможных исков со стороны правообладателей. Благодаря патентной аналитике возможно осуществить в том числе сбор и анализ информации о контрагентах, с которыми выгодно вести гражданско-правовые отношения, осуществлять совместные разработки в той нише на рынке, где компания собирается развиваться. Также по истории изменения статуса, судебных дел и заключенных договоров по выданным патентам можно проследить историю успехов и неудач конкурентов, рассмотреть предметно факты неправомерного использования патентов компании или интересующих ее направлений для дальнейших инновационных разработок. Это позволит понять какая форма правовой охраны является наиболее привлекательной, какие ошибки при составлении формул совершаются конкурентами и что наиболее ценится потенциальными лицензиатами [9].

В целях апробации приведенных тезисов в рамках настоящего исследования проведен анализ патентной ситуации в сфере цифровых технологий на примере аддитивного производства (послойного синтеза). В рамках проведенного исследования была изучена патентная документация в области техники, соответствующей

группе международного патентного классификатора (МПК) В 33У «Технология послойного синтеза, т. е. изготовление трехмерных (3D) объектов добавочным нанесением, добавочной агломерацией или добавочным наслоением, например, посредством 3D-печати, стереолитографии или избирательного лазерного спекания». Для ее анализа применялись инструмент патентной аналитики Orbit intelligence от компании Questell и методы описательной статистики. В настоящее время технологии цифрового аддитивного производства являются популярными и применяются в различных отраслях промышленности. В результате анализа зарегистрированных в РФ патентных документов, полученных как от отечественных заявителей, так и от иностранных компаний, все найденные документы были сгруппированы по патентным семействам, где одно семейство включало в себя совокупность всех патентных публикаций, относящихся к одному изобретению или полезной модели. Выяснилось, что в РФ за последние двадцать лет патентная активность в рассматриваемой сфере послойного синтеза только увеличивалась, вплоть до наступления ковидных ограничений в 2020 г. При этом пик активности иностранных заявителей пришелся на 2016–2017 гг., а отечественные заявители проявили активность в патентовании технических решений в данной области лишь спустя пару лет в 2018–2020 гг., когда иностранные заявители сбавили свою активность на нашем рынке (рис. 1).

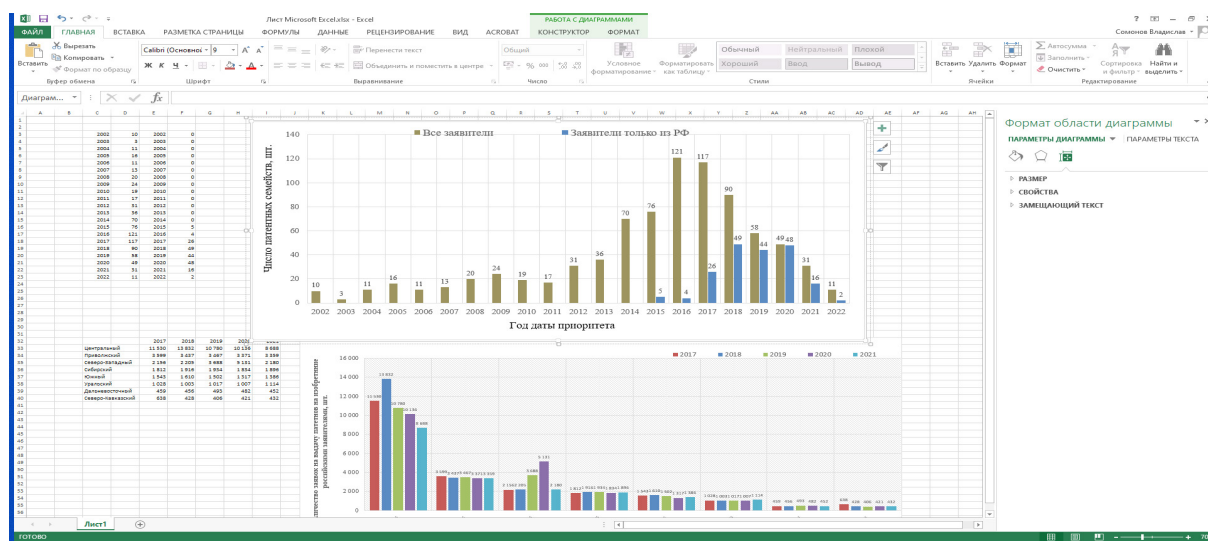


Рис. 1. Динамика патентной активности в сфере послойного синтеза в РФ (разработано авторами на основе [3])

В результате исследований российской патентной коллекции [10] удалось определить, что на протяжении последних пяти лет лидером среди регионов по патентной активности является Центральный федеральный округ, а также Приволжский федеральный округ, который лишь в 2020-е гг. уступил второе место Северо-Западному (рис. 2).

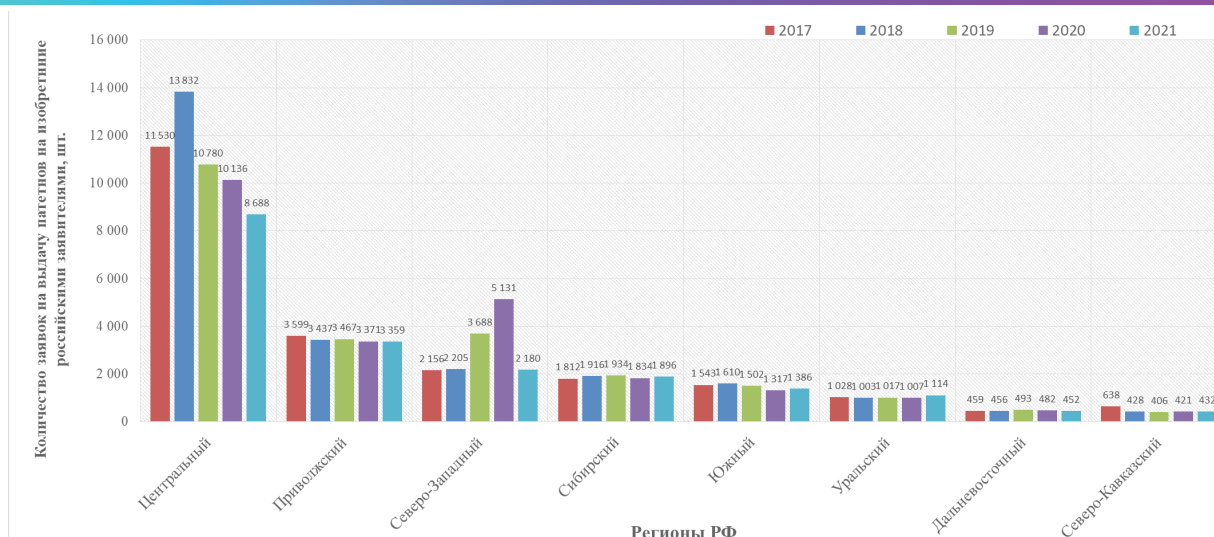


Рис. 2. Динамика патентной активности российских заявителей, по федеральным округам Российской Федерации в период 2017–2021 гг. (разработано авторами на основе [10])

Это же лидерство отечественных правообладателей из Центрального федерального округа наблюдается и в сфере аддитивного производства (рис. 3), за ним следуют Приволжский и Южный округа, что подтверждает гипотезу о том, что большая часть исследований отечественной науки в этом направлении проводится в Москве.



Рис. 3. Ведущие российские правообладатели в сфере аддитивного производства в период 2016–2022 гг. (разработано авторами на основе [3])

В ходе исследований выяснилось, что правообладатели из Москвы активно патентовали свои разработки в основном в период с 2017 по 2019 гг., среди изобретателей лидирует Д. Л. Сапрыкин, а затем в лидеры вышел Казанский национальный исследовательский университет во главе с Р. Х. Мухаметрахимовым (рис. 4). Это говорит о том, что региональные вузы в последние годы тоже получили финансирование исследований в данной области, что дало толчок в создании новых технических решений и они становятся серьезными конкурентами столичных компаний на отечественном рынке и с их разработками стоит считаться при выводе своей продукции на рынок, а среди отечественных изобретателей появляются

ся ведущие творческие коллективы (Манн, Крохин, Королев-АО «РУСАЛ Урал», отец и сын Сапрыкины – МГТУ Станкин), которых компании стоит переманивать в свои ряды для развития данных технологий.

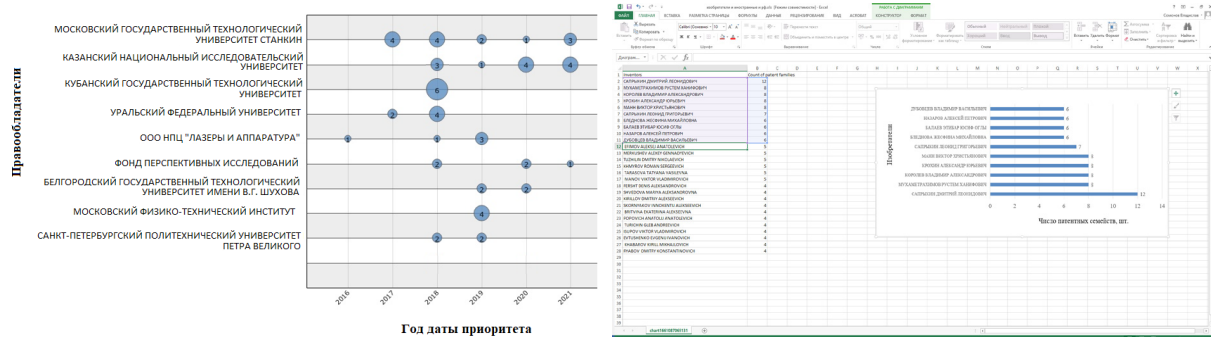


Рис. 4. Патентная активность российских правообладателей и лидеры среди отечественных изобретателей сфере аддитивного производства в период 2016–2021 гг. (разработано авторами на основе [3])

В рамках настоящего исследования были выявлены основные сферы применения запатентованных отечественными разработчиками решений (рис. 5).

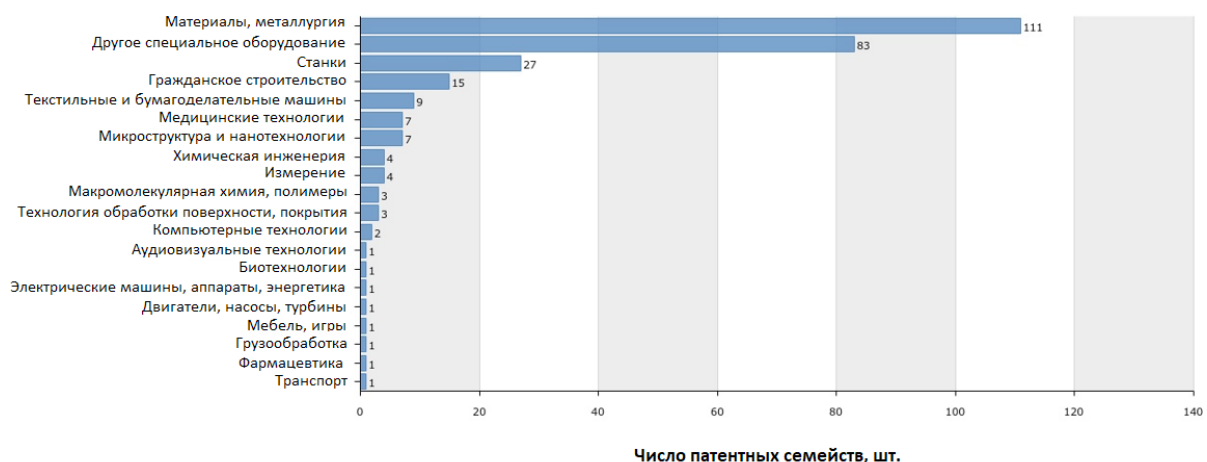


Рис. 5. Основные сферы применения запатентованных решений отечественными разработчиками в сфере аддитивного производства в период 2015–2022 гг. (разработано авторами на основе [3])

Из рисунка видно, что в основном решения патентуются в области материалов, металлургия и специализированного оборудования для аддитивного производства. При патентовании своих решений отечественные лидеры в основном ссылаются на ближайших конкурентов (Московский государственный университет Станкин на Уральский федеральный университет, ООО НПЦ «Лазеры и аппаратура» на Фонд перспективных исследований). Это свидетельствует об их тесном сотрудничестве, либо о значимости их разработок для ближайших конкурентов.

Безопасность инновационного бизнеса в значительной степени зависит от наличия у компании возможности запатентовать свои разработки в других странах. Это позволит при обнаружении факта неправомерного использования разработок компании предъявить иск на территории тех стран где существует соответствующая правовая охрана и избежать откровенного вывоза разработок компании за рубеж в результате промышленного шпионажа. В этом вопросе у ведущих отечественных правообладателей в сфере послойного синтеза были выявлены проблемы в связи с патентованием технических решений только в нашей стране, в отличие от зарубежных, которые сначала патентуются в ведущих странах мирового рынка аддитивного производства, а уже потом выходят на наш рынок (рис. 6). Из рисунка также видно, что самыми крупными патентными портфелями в данной области в нашей стране обладают иностранные компании из Германии (DWS), США (Boeing, Xerox) и Франции (Safran aircraft engines). Это значительно затрудняет развитие данной отрасли внутри страны.

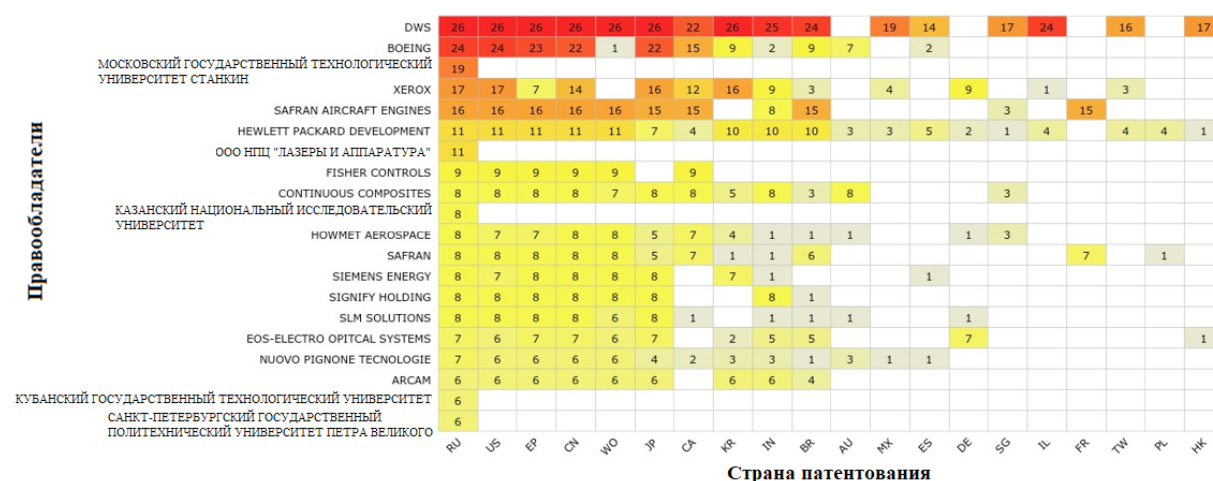


Рис. 6. Патентование ведущих правообладателей в области послойного синтеза в период 2002–2021 гг. в РФ по странам мира (разработано авторами на основе [3])

Также отечественные разработчики не уделяют должного внимания коммерциализации своей интеллектуальной собственности через лицензирование прав на полученные патенты, о чем свидетельствуют данные об отсутствии заключенных у отечественных правообладателей в данной сфере лицензионных договоров.

Российские правообладатели недостаточно эффективно используют современные инструменты патентования. Регистрация патентных прав на разработки только на территории нашей страны создает пространство для возникновения на зарубежных рынках конкурирующих продуктов, которые не охраняются в данных юрисдикциях, а значит, могут быть свободно использованы. При таком подходе высокое качество российских патентных заявок, которое демонстрируют заявители в данном сегменте играет против отечественных производителей, которые самостоятельно усиливают позиции глобальных конкурентов, используя патентова-

ние только как международный институт депонирования собственного авторства, а не как механизм приобретения монопольных прав на созданную технологию.

Развитие промышленного производства на основе применения инструментария патентной аналитики позволит формировать сильные региональные центры компетенций, в которых производители будут иметь ресурсы для производства качественного и конкурентного продукта, при этом смогут охранять его не только на территории нашей страны, но за рубежом на наиболее перспективных рынках. Считаем необходимым включение мероприятий патентной аналитики в состав комплекса мер обеспечения технологического суверенитета Российской Федерации.

Заключение. Проблемы информационной безопасности и получения необходимой информации о конкурентах и их разработках сегодня особенно актуальны в стремительно развивающемся цифровом производстве. Ведь благодаря своевременно полученной информации можно предвидеть риски и минимизировать их пагубное влияние на деятельность компании. Одним из действенных инструментов для снижения рисков при инновационном развитии компании и своевременного реагирования на изменения ситуации на рынке является патентная аналитика.

В результате исследований были выявлены проблемы недостаточной грамотности сотрудников исследовательских подразделений в области интеллектуальной собственности и пренебрежительное отношение к результатам интеллектуальной деятельности. На примере послойного синтеза было показано, как применение патентной аналитики позволяет определить текущие ключевые направления для патентования, выбрать перспективные области для инновационных разработок, определить лидеров рынка и потенциальных конкурентов, стратегии их правовой охраны своих разработок, выявить момент для беспрепятственного использования основных технических решений в данной области в своих целях на территории РФ.

На сегодняшний день конкуренция в данной области цифрового производства в нашей стране увеличивается. Для принятия своевременных и правильных управленческих решений, минимизации возможных последствий от разглашения существенной информации и наличия, блокирующих деятельность компании патентов, возникает необходимость с применением патентной аналитики постоянного мониторинга не только нарушения патентов компании, но поиска новых перспективных ниш на рынке для дальнейшего развития и удержания своей позиции на рынке.

Список литературы

1. Гришина С. В. Патентный анализ как инструмент стратегической диагностики // Научно-технические ведомости СПбГПУ. Экономика и менеджмент предприятия. 2008. № 1. С. 113–115.
2. Ильина И. Е., Золотых Н. И., Биткина И. В. Патентная активность региона как драйвер развития экономики России // Управление наукой и наукометрия. – 2022. Т. 17, № 1. С. 10–35.
3. Информационный web сайт компании orbit: Сервер платной патентной базы Orbit Intelligence компании Questel. URL: <https://www.orbit.com/> (дата обращения: 29.08.2022).

4. Николаев А. С. Ключевые подходы к определению роли патентной аналитики в процессе организации и стимулирования инновационной деятельности. // *Инновации*. 2019. № 12 (254). С. 119–123.
5. Николаев А. С. Патентная аналитика: учебно-методическое пособие / А. С. Николаев. Санкт-Петербург: Университет ИТМО, 2022. 98 с.
6. Николаев А. С., Бузмакова А. А. Построение инновационного ландшафта голосового ассистента // *Экономика. Право. Инновации*. 2020. № 4. С. 81–88.
7. Паап Д. Картирование технологического ландшафта для ускорения инноваций // *Форсайт*. 2020. Т. 14, № 3. С. 41–54.
8. Путин В. В. Взаимодействие науки и бизнеса должно стать ключевым условием реализации программы цифровой экономики // *Роспатент*. URL: <https://rospatent.gov.ru/ru/news/putinnauka/> (дата обращения: 10.08.2022).
9. Стерхов А. П. Использование маркетинговых технологий для обеспечения безопасности инновационного бизнеса // *Вестник ИрГТУ*. 2013. № 7 (78). С. 206–214.
10. Суконкин А. В., Иванова М. Г., Александрова А. В., Аникеева М. Ю., Александров Ю. Д., Евстратова А. С., Завгородняя Ю. В. Аналитические исследования сферы интеллектуальной собственности 2021: коэффициент изобретательской активности в регионах Российской Федерации. М.: Федеральный институт промышленной собственности (ФИПС), 2022. 59 с.
11. Ena O. ‘Domain-specific’ patent analytics: Focus on company’s technology priorities // *World Patent Information*. 2021. Volume 65, 102037.
12. Fortune business insights. Market research Report FBI102774. 2021. URL: <https://www.fortunebusinessinsights.com/patent-analytics-market-102774> (дата обращения: 10.08.2022).
13. Pantano El., Priporas C. V., Sorace St., Iazzolino G. Does innovation-orientation lead to retail industry growth? Empirical evidence from patent analysis // *Journal of Retailing and Consumer Services*. 2017. Volume 34. Pp. 88–94.

Н. В. Спешилова,

доктор экономических наук, профессор,
Оренбургский государственный университет

А. А. Мамедов,

студент,
Оренбургский государственный университет

ВЫГОДЫ, РИСКИ, ПРОБЛЕМЫ И МАСШТАБЫ ЦИФРОВИЗАЦИИ

Аннотация. В статье представлены преимущества внедрения процессов цифровизации в различные сферы производства и жизнедеятельности человека. Сформулированы связанные с этим риски и проблемы, возникающие на сегодняшний день, в том числе в сферах законодательства и подготовки высококвалифицированных кадров. Сделан акцент на криптовалюте и майнинге. Представлен

вывод, что для масштабирования процессов цифровизации в России необходимо уделять внимание не только техническому и технологическому обеспечению, но и законодательной базе, а также формированию соответствующего уровня образования как разработчиков программного обеспечения, так и пользователей.

Ключевые слова: цифровизация, IT-технологии, криптовалюта, биткоин, торговля и майнинг, законодательство, кадры, экономика

BENEFITS, RISKS, PROBLEMS AND SCALE OF DIGITALIZATION

Abstract. The article presents the advantages of introducing digitalization processes into various spheres of production and human activity. The risks and problems associated with this are formulated, which arise today, including in the areas of legislation and training of highly qualified personnel. Emphasis is placed on cryptocurrency and mining. The conclusion is presented that in order to scale the digitalization processes in Russia, it is necessary to pay attention not only to technical and technological support, but also to the legislative framework, as well as to the formation of an appropriate level of education for both software developers and users.

Keywords: Digitalization, IT technologies, Cryptocurrency, Bitcoin, Trading and mining, Legislation, Personnel, Economy

Благодаря цифровизации запущены процессы упрощения и автоматизации функционирования различных сфер бытовой жизни и производства посредством внедрения современных технологий.

Глобальная цифровизация касается практически всех сфер жизнедеятельности, общества, реализуется повсеместно, без исключений – все компании в той или иной мере внедряют в свою жизнь и работу цифровые технологии [5, 6, 9]. Безусловно, данный процесс влечет за собой экономию и оптимизацию временных и трудовых затрат на обработку информации, документации и т. д. Среди выгод цифровизации можно выделить: увеличение производительности труда; появление новых компаний на рынке, что в свою очередь привело, с одной стороны к росту конкуренции, а с другой – к увеличению числа вакансий на рынке труда (и как следствие уменьшение безработицы и социального неравенства); снижение издержек производства.

Однако имеют место и риски, связанные с неграмотностью в сфере IT-технологий, недостатком самой IT-инфраструктуры, большим спросом на специалистов в этой сфере, превышающим имеющиеся предложения.

Для минимизации потенциальных рисков при внедрении цифровых процессов необходим комплексный подход, одно из направлений которого – внесение изменений в систему образования с целью повышения грамотности использования IT-технологий, в том числе с точки зрения безопасности (например, в период школьного (и даже дошкольного) образования посредством введения соответствующего предмета в школе, поскольку использование гаджетов практикуется с самого детства). Работа в сфере IT-технологий позволяет ее реализацию в удаленном дистанционном формате, однако подготовке специалистов, востребованных на региональных трудовых рынках, также следует уделять существенное внимание [3].

Можно выделить три главных направления цифровизации.

1. Промышленная. Цифровизация промышленности – это концепция нового цифрового пространства, единая система, в которой производственные машины, системы гарантируют безопасность компании (сенсоры и датчики позволяют комбинировать различные физические объекты в виртуальной сети, где они могут передавать информацию между собой без вмешательства человека) [6]. Главное преимущество – производительность (компания сокращает время, необходимое для разработки нового продукта, его вывод на рынок и доставку потребителю), а также оптимизация ресурсов предприятия, что повышает эффективность его работы в целом. Сегодня имеет место реальная потребность в оцифровке промышленных предприятий, так как существует проблема обработки огромных массивов данных на различных заводах и производствах. Современные технологии дают возможность не только автоматизировать машины, но и взаимодействовать между собой в разных сферах работы предприятия.

2. Бытовая цифровизация. Это не менее значимая категория, к которой можно отнести такие системы, как «умный дом», «умный город», госуслуги, запись к врачу через Интернет, оповещения о каких-то чрезвычайных происшествиях через систему рассылки СМС-сообщений, QR-коды, роботы-курьеры (доставка еды, посылок и пр.).

Так, если говорить о технологии «умный дом» [8], то, например, «умное» освещение можно реализовать тремя способами: установкой проводных выключателей света в стены; использованием интеллектуального штекера с поддержкой приложений; разработкой индивидуального проекта «умного освещения». При длительном отсутствии человека (отпуск, командировка и пр.) система имитирует присутствие хозяев, периодически включая/выключая свет в доме, что отпугивает злоумышленников и предотвращает вторжение, обеспечивая дополнительный уровень поддержки системе охранной сигнализации. Кроме того, «умный дом» использует систему освещения для реагирования на различные ситуации в доме (например, свет начнет мигать, если сработает детектор дыма, или ландшафтные светильники автоматически включатся, когда сядет солнце). «Умное» освещение обычно устанавливается в нескольких комнатах. Это дает возможность значительной экономии электроэнергии в масштабах всего дома. В долгосрочной перспективе снижение затрат от управления освещением приводит к уменьшению потребления энергии, что достигается за счет комплексного использования всей системы: датчиков, элементов управления, логики и «умных» алгоритмов; светодиодного освещения. Кроме того, «умные» диммеры регулируют интенсивность светового потока в зависимости от предпочтений хозяина, его активности или времени суток. Они уменьшают мощность источника света, чтобы сэкономить энергию и продлить срок службы ламп.

3. Криптовалюта. Это любая валюта в цифровом формате, причем транзакции защищены посредством шифрования. Не существует центрального органа по выпуску или регулированию криптовалют. Для записи транзакций и выпуска новых единиц используется децентрализованная система.

Главное отличие криптовалюты от обычной валюты: не существует никаких центральных органов по выпуску, никакого контроля. Не подразумевается опера-

ций с физическими деньгами, имеющими хождение и возможности обмена в реальном мире. Название «криптовалюта» вошло в использование вследствие того, что в транзакциях используется шифрование, а именно криптография. Главная цель криптовалюты – надежность и безопасность транзакций любого характера [7]. В 2009 г. появилась первая криптовалюта – биткойн.

На бирже можно увидеть множество различных криптовалют. Наиболее популярные: биткойн (Bitcoin) – самая известная и самая ценная в наше время; эфириум (Ethereum) – при оплате в сети имеет более быстрое подтверждение транзакции в отличие от биткойна, в цене намного меньше, чем биткойн; литкойн (Litecoin) – имеет очень много нововведений относительно своих собратьев, выгодное хранение денег в этой валюте.

Последнее время все более актуальным становится вопрос, как безопасно купить криптовалюту. Есть два способа: торговля и майнинг.

Рассмотрим торговлю криптовалютой:

– первый шаг – подбираем более удобную платформу для использования. При этом есть выбор из двух вариантов: брокер или специализированная биржа для торговли криптовалютами (брокер – человек, предлагающий покупку и продажу криптовалюты, различных активов, облигаций за небольшой процент от сделанной им выручки; специализированная биржа – в интернете их огромное количество, отличаются комиссиями за операции);

– второй шаг – пополнение счета, чтобы начать торговать. Сделать это можно при помощи дебетовой или кредитной карты. Счет на бирже может быть пополнен любым онлайн-методом, удобным для пользователя, в случае работы с брокером, он может подсказать, как это сделать. Одним из важнейших факторов, который нельзя упускать, является размер комиссий за зачисление и вывод средств, а также торговые комиссии. Это необходимо изучать еще на первом этапе;

– третий шаг – размещение заказа на приобретение определенного количества криптовалюты – сделать это можно также через брокера или же непосредственно на бирже (аналогично размещается лот на продажу).

Что касается майнинга (от англ. mining – добыча полезных ископаемых), то это процесс «добычи» криптовалюты, виртуальных денег, эмиссия которых никем не регулируется [4]. Процесс работает благодаря технологии блокчейн – цепочке блоков, каждый из которых хранит информацию об отдельной транзакции. Работоспособность блокчейна напрямую зависит от вычислительных мощностей компьютеров, подключенных к цепочке. Все участники блокчейна хранят всю цепочку блоков с самого начала, постоянно добавляя новые блоки в конец. Майнеры занимаются сбором и обработкой информации о всех операциях, которые в данный момент происходят с криптовалютой [4]. Сейчас майнинг криптовалюты невозможен без специального дорогого оборудования. Существуют промышленные майнинг-фермы – они могут состоять из 30–50 майнеров, а могут быть гигантскими и включать в себя десятки тысяч устройств [1, 4].

Однако майнинг – это очень энергозатратное занятие. Поэтому его эффективность сильно зависит от стоимости электроэнергии. Так, например, в России стоимость электричества значительно ниже, чем в европейских странах [2]. Если же дата-центр будет находиться на территории электростанции или в особой экономической зоне

со специальными условиями на покупку электроэнергии, гарантированными государством, то это позволит законно значительно сэкономить на электричестве.

Второй фактор, влияющий на комфортность и прибыльность майнинга, – общая температура. Майнинговые мощности выделяют огромное количество тепла, и, чем прохладнее климат, тем меньше необходимо затрат на кондиционирование и вентиляцию. Поэтому большинство крупных дата-центров находятся в северной части России и даже в Арктике. Климатические условия России делают майнинг выгоднее [2].

Однако из-за несовершенства законодательной базы участились рейдерские захваты майнингового оборудования на основании якобы неверно оформленных документов на право деятельности дата-центров. До последнего времени майнинг и криптовалюты почти никак не регулировались и практически находились в серой зоне. Но со вступлением в силу с января 2021 г. Федерального закона о цифровых финансовых активах (ЦФА), появилась перспектива выхода рынка из тени. На данном этапе в документах пока превалирует скорее карательная направленность, чем позитивная мотивация. Закон содержит неоднозначные формулировки о майнинге, не позволяющие признать эту деятельность выпуском цифровой валюты. Есть вероятность трактовки майнинга как услуги, а получение криптовалюты – оплатой таких услуг, что нарушит прямой запрет закона о ЦФА [2]. Но есть надежда, что спорные моменты будут решены.

Криптовалютный рынок очень волатилен, поэтому возможны резкие колебания цен на валюты. Сегодня он все еще находится на этапе становления, а сама валюта считается весьма спекулятивной. Однако следует внимательно следить за тенденциями в части актуальных изменений, в том числе в законодательной сфере. При этом нет смысла вкладывать все средства в биткоин только потому, что это название на слуху. Есть огромное количество вариантов инвестирования, и лучше распределить средства по нескольким валютам.

Выводы. Подводя итог вышесказанному, следует отметить, что цифровизация проникает во все сферы жизнедеятельности современного человека, оказывая влияние на развитие мировой экономики. Данная тенденция все более усиливается и требует не только технического и технологического обеспечения, но соответствующей законодательной базы, а также уровня образования как разработчиков программного обеспечения, так и пользователей.

Список литературы

1. В сети показали самую крупную майнинг-ферму в Казахстане и СНГ – она «кушает» электричество как целый город // Официальный сайт Клуб DNS. URL: <https://club.dns-shop.ru/digest/58901-v-seti-pokazali-samuu-krupnuu-maining-fermu-v-kazahstane-i-sng/> (дата обращения: 24.07.2022).
2. Кожеваткин В. К., Гербель М. И., Чаплагина С. С. Майнинг в России: угрозы и перспективы развития // Научные исследования XXI века. 2021. № 5 (13). С. 24–29. URL: <http://elibrary.ru/item.asp?id=47185557> (дата обращения: 24.07.2022).
3. Мажарова Н. А., Спешилова Н. В., Андриенко Д. А. Проблемы формирования высококвалифицированных кадров для экономики региона в условиях цифровизации (на примере Оренбургской области) // Труд и социальные отношения. 2020. Т. 31, № 1. С. 84–100. DOI: 10.20410/2073-7815-2020-31-1-84-100

4. Майнинг: как добывается криптовалюта, почему это опасно для экологии // РБК Тренды. URL: trends.rbc.ru/trends/education/6163fa3f9a79472472bca0d3 (дата обращения: 14.06.2022).

5. Огородников П. И., Спешилова Н. В. Инновации и инвестиции в процессах цифровизации сельскохозяйственного производства в регионе // Научное обозрение: теория и практика. 2021. № 3 (83). С. 706–717. DOI: 10.35679/2226–0226–2021–11–3–706–717

6. Цифровизация промышленности // Официальный сайт ООО «Центр 2М». URL: <https://center2m.ru/tsifrovizatsiya-promishlenosti> (дата обращения: 12.07.2022).

7. Что нужно знать о криптовалюте // Журнал для инвесторов АО «ААА Управление Капиталом». URL: <https://www.gpb-am.ru/press-center/journal/65-chto-nuzhno-znat-o-kriptovaliute> (дата обращения: 14.06.2022).

8. Что такое «умный» дом, из чего он состоит и зачем нужен // РБК Тренды. URL: <https://trends.rbc.ru/trends/industry/606d99c19a7947b14fe9c2d6> (дата обращения: 24.07.2022).

9. Shepel V. N., Speshilova N. V., Kitaeva M. V. Technology Of Management Decision-Making At Industrial Enterprises In The Digital Economy // International Scientific Conference “Global Challenges and Prospects of the Modern Economic Development” (Samara State University of Economics, Samara, Russia 6–8 December, 2018) // The European Proceedings of Social & Behavioural Sciences EpSBS. Vol. LVII – GCPMED 2018. Pp.1520–1531. URL: <https://www.futureacademy.org.uk/files/images/upload/GCPMED%202018F155.pdf> DOI: <https://dx.doi.org/10.15405/epsbs.2019.03.155>

Д. В. Степаненко,
магистрант,

Уральский федеральный университет имени первого Президента России
Б. Н. Ельцина

СРАВНИТЕЛЬНЫЙ ОБЗОР МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ИЗ МЕТОДИКИ ФСТЭК РОССИИ И МАТРИЦ MITRE ATT&CK

Аннотация. В статье проводится сравнительный анализ приемов и подходов моделирования угроз безопасности информации из действующей методики ФСТЭК России и матриц MITRE ATT&CK, отмечаются преимущества и недостатки методик оценки угроз. Кратко рассмотрен фреймворк ATT&CK на примере «технологических доменов» с групповой классификацией связанных действий. Уделено внимание документу «Модель угроз» как важного результирующего документа при создании системы защиты информации по требованиям регулятора. Предложены направления исследований по автоматизации оценки актуальных угроз и уязвимостей. Кроме того, поднят вопрос о проведении компаративного анализа рассматриваемых методик.

Ключевые слова: моделирование угроз, УБИ, ФСТЭК России, матрица MITRE ATT&CK, информационная безопасность, угроза безопасности информации, уязвимость, оценка актуальности угроз, банк данных угроз

COMPARATIVE REVIEW OF INFORMATION SECURITY THREAT MODELING FROM THE FSTEC METHODOLOGY AND MITRE ATT&CK MATRICES

Abstract. The article provides a comparative analysis of techniques and approaches for modeling information security threats from the current FSTEC methodology and MITRE ATT&CK matrices, the advantages and disadvantages of threat assessment methods are noted. The ATT&CK framework is briefly considered on the example of “technological domains” with a group classification of related actions. Attention is paid to the document “Threat Model” as an important resulting document when creating an information protection system according to the requirements of the regulator. The directions of research on automating the assessment of current threats and vulnerabilities are proposed. In addition, the question of conducting a comparative analysis of the methods under consideration was raised.

Keywords: Threat modeling, FSTEC, MITRE ATT&CK matrix, Information security, Information security threat, Vulnerability, Threat relevance assessment, Threat data bank

Матрицы MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge – «сопоставительные тактики, техники и общеизвестные факты о злоумышленниках») – глобально доступная база знаний о тактике и методах злоумышленников, основанная на реальных наблюдениях; с течением времени ставшая распространенной методологией оценки угроз безопасности информации (УБИ) среди специалистов по информационной безопасности (кибербезопасности).

MITRE – некоммерческая организация в США, основной деятельностью которой является управление различными центрами исследований и разработок. В рамках исследований в области кибербезопасности в интересах мирового сообщества MITRE имеет более чем 50-летнюю историю разработки стандартов и инструментов, используемых широким сообществом специалистов по кибербезопасности [12].

Благодаря таким фреймворкам, как ATT&CK, Engage, D3FEND и CALDERA, а также множеству других инструментов по кибербезопасности, MITRE «вооружает» мировое сообщество специалистов уникальными продуктами по моделированию УБИ и противостоянию им.

В сфере кибербезопасности корпорация MITRE известна с 1999 г. Тогда была представлена одна из первых в мире база данных общеизвестных уязвимостей информационной безопасности в виде списка CVE (Common Vulnerabilities and Exposures). С тех пор эта структурированная база данных, которая стандартизировала описательный подход к определению уязвимостей, стала одним из основных ресурсов, где хранят данные по уязвимостям в системном и прикладном программном обеспечении [4].

В 2013 г. MITRE представила матрицы ATT&CK, реализованные в виде фреймворка, как способ описания поведенческой модели нарушителей на основе реальных наблюдений для составления структурированной матрицы используемых злоумышленниками приемов, чтобы упростить задачу реагирования на инциденты [11].

Фреймворк АТТ&СК, который представляет собой бесплатную онлайн-базу знаний о поведении нарушителей, используется по всему миру. АТТ&СК помогла внедрить концепцию защиты с учетом угроз, которая использует глубокое понимание методов и технологий нарушителя для защиты от кибератак, их обнаружения и смягчения. Собирая профиль нарушителя и его возможных действий, удается понять, какие инструменты используются, ознакомиться с их техниками и тактиками. В итоге, построив поведенческий паттерн злоумышленника, можно спрогнозировать вероятную «точку входа» в организации [10].

АТТ&СК находится в свободном доступе для всех, включая частный сектор, правительства и профессиональные сообщества продуктов и услуг по защите информации, что сильно упрощает разработку конкретных моделей угроз и методологий. База знаний АТТ&СК описывает общие тактики, техники (методы) и процедуры, используемые киберпреступниками. При этом АТТ&СК предоставляет специалистам по кибербезопасности общий язык для обсуждения возникающих угроз и разработки эффективных стратегий защиты.

Наряду с матрицей АТТ&СК для организаций, MITRE также предоставляет конкретные рекомендации для облачных сервисов, ОС Windows, ОС Linux, ОС macOS, мобильных и промышленных систем управления.

АТТ&СК описывает поведение на протяжении всего жизненного цикла реализации УБИ, обычно известное как тактика, техника и процедуры (так называемые наборы ТТР – tactics, techniques, и procedures). В АТТ&СК это поведение соответствует трем более детализированным уровням [13. С. 2]:

1. **Тактика** представляет собой «что» и «почему». Это технические цели нарушителя, причина выполнения действия и то, чего он пытается достичь. Каждая тактика содержит множество приемов, которые, по наблюдениям специалистов, используются в обычной деятельности субъектами угроз.

2. **Техники** представляют собой «как» нарушитель достигает тактической цели, выполняя действие. Техники могут также представлять то, что нарушитель получает, выполняя действие. Техника – это конкретное поведение для достижения цели, и часто это один шаг в череде действий, направленных на выполнение общей цели нарушителя.

3. **Процедуры** – это конкретные примеры того, как была использована техника. Они могут быть полезны для репликации инцидента с эмуляцией нарушителя и для получения подробной информации о том, как обнаружить этот используемый экземпляр. Фреймворк АТТ&СК организован в виде серии так называемых «технологических доменов» – экосистем, в рамках которых действует нарушитель. Ниже приведены базы знаний АТТ&СК для конкретных областей, которые были разработаны или разрабатываются в настоящее время [12]:

1. **MITRE АТТ&СК – Enterprise:**

- для ОС Windows, Linux, и MacOS;
- облачные сервисы AWS, GCP, Azure, Office 365, Azure AD, SaaS;
- управление сетевой инфраструктуры.

2. **MITRE АТТ&СК – Mobile:** модель состязательных тактики и техник для получения доступа к платформам Android и iOS.

3. MITRE ATT&CK – Industrial Control Systems (ICS): фокусируется на тактике и техниках нарушителя, основной целью которого является нарушение процесса эксплуатации АСУ ТП, включая системы диспетчерского управления и сбора данных (SCADA).

Чтобы выделить используемые тактики, техники и процедуры, например, после анализа вредоносной программы или недеklarированных возможностей программного обеспечения, можно воспользоваться MITRE ATT&CK Navigator. Для автоматизации маппинга (взаимного сопоставления полей данных) можно использовать официальный инструмент Threat Report ATT&CK Mapper (TRAM). Для моделирования (симуляции) кибератак (Adversary Simulation Tools) можно использовать свободно распространяемую утилиту MITRE CALDERA.

Кроме того, для быстрого принятия решений в фреймворке ATT&CK реализована групповая классификация связанных действий [11]. Группы рассматриваются в виде наборов связанных действий нарушителя, которые отслеживаются по условному общему имени. При работе с такими группами аналитики отслеживают кластеры действий, используя различные аналитические методологии и термины, такие как группы угроз, группы действий, субъекты угроз, наборы вторжений и кампании.

Некоторые группы имеют несколько названий, связанных с аналогичными действиями, из-за того, что различные организации отслеживают аналогичные действия под разными именами. Определения групп организаций могут частично совпадать с определениями групп, определенными другими организациями, но могут не совпадать в отношении конкретной деятельности.

Для удобства использования связанных групповых страниц, представленных в табличной форме с множеством ссылок не те или иные атрибуты, команда MITRE ATT&CK использует термин «Группа» для обозначения любого из вышеперечисленных обозначений кластера действий нарушителя. Кроме того, постоянно ведется корреляционный анализ данных для отслеживания совпадений между именами на основе общедоступных ассоциаций, которые обозначаются как «Связанные группы» на каждой странице, поскольку эти совпадения могут быть полезны для осведомленности аналитиков и специалистов по кибербезопасности.

Группы сопоставляются с использованием общедоступных техник, о которых сообщается в контексте анализа, и включаются оригинальные ссылки. Выходная информация представляет не все возможные техники, используемые Группами, а скорее подмножество, доступное исключительно через отчеты с открытым исходным кодом. Группы также сопоставляются с используемым программным обеспечением. Использование техник для этого программного обеспечения отслеживается отдельно на каждой странице.

Таким образом, MITRE внесла значительный вклад в развитие сообщества кибербезопасности, представив базу знаний ATT&CK и связанные с ней инструменты и ресурсы. Поскольку нарушители постоянно находят способы действовать все более скрытно и избегать обнаружения с помощью традиционных средств обеспечения безопасности, специалистам приходится менять свой подход к обнаружению и защите [3. С. 8].

Профессиональное сообщество специалистов по кибербезопасности, приверженцев идеологии MITRE ATT&CK, с каждым годом увеличивается, поэтому и применение этого фреймворка становится очень востребованным. К примеру, вендоры используют ATT&CK для создания меток безопасности в своих программных продуктах. Кроме того, данный фреймворк можно использовать для выявления пробелов в защите, оценки возможностей средств обеспечения безопасности, организации обнаружения, поиска угроз, участия в мероприятиях STF/RedTeam или для проверки средств контроля за смягчением последствий. Это качественно упрощает расследование инцидентов и реагирование на них.

Как отмечает Агентство по кибербезопасности и защите инфраструктуры США (CISA), понимание поведения злоумышленников часто является первым шагом в защите данных [13. С. 19]. Успех в обнаружении и смягчении последствий кибератак зависит от этого понимания. Это послужило точкой отсчета тесного сотрудничества между CISA и командой MITRE и впоследствии для выбора фреймворка ATT&CK в качестве основы для разработки конкретных моделей угроз и методологий разработчиков средств обеспечения кибербезопасности в надежде стандартизировать отрасль [13. С. 3]. Другими словами, CISA использует ATT&CK в качестве «объектива», через который можно идентифицировать и анализировать поведение нарушителя.

Матрицы MITRE ATT&CK предоставляет подробную информацию о более чем 100 группах субъектов угроз, включая методы и программное обеспечение, которые, как известно, они используют (примечание: не каждое поведение злоумышленника задокументировано в ATT&CK!). Но однозначно можно утверждать, что с созданием ATT&CK и, разумеется, с постоянной актуализацией базы данных фреймворка, MITRE выполняет свою миссию по решению проблем для более безопасного мира – объединяя профессиональные сообщества для разработки более эффективных мер кибербезопасности [11].

Так как матрица ATT&CK представляет собой обширное описание поведения злоумышленника, данный фреймворк может быть полезен для различных наступательных и защитных измерений, представлений и других механизмов (например, в процессе оценки УБИ по методике ФСТЭК России).

В Российской Федерации регулятивные правовые функции по технической защите информации возложены на Федеральную службу по техническому и экспортному контролю (ФСТЭК России). Кроме того, являясь федеральным органом исполнительной власти, ФСТЭК России осуществляет реализацию государственной политики и контрольные функции в области государственной безопасности по вопросам:

- обеспечения безопасности критической информационной инфраструктуры;
- противодействия техническим разведкам;
- защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- осуществления экспортного контроля.

5 февраля 2021 г. ФСТЭК России утвержден методический документ «Методика оценки угроз безопасности информации» (Методика-2021) [5. С. 1],

который определяет порядок моделирования и оценки актуальности угроз и возможные сценарии их реализации в информационных системах на основе Банка данных угроз безопасности информации (БДУ) ФСТЭК России [1].

Разработка модели угроз безопасности информации, как главного результирующего документа, структура которого также регламентируется Методикой-2021, при создании системы защиты информации является важнейшим этапом формирования требований по техническим и организационным мерам защиты информации в процессе последующего проектирования и реализации системы защиты информации [8. С. 7].

Модель угроз стоит рассматривать как формализованное (структурированное) описание УБИ для конкретной информационной системы (ИС) или группы информационных систем в определенных условиях их функционирования.

Модель угроз содержит:

- описание ИС и ее структурно-функциональных характеристик;
- описание УБИ в комплексе (возможности нарушителей, возможные уязвимости, способы реализации УБИ, последствия от нарушения свойств безопасности информации – «конфиденциальность, целостность, доступность»).

При разработке модели угроз необходимо учитывать требования Приказа ФСТЭК России № 17, которые являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах. Данные требования предназначены для обладателей информации, заказчиков, заключивших государственный контракт на создание государственной информационной системы и операторов государственных информационных систем [8. С. 5–7].

Для определения УБИ и разработки модели УБИ применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 [9].

Таким образом, составление модели угроз основывается, прежде всего, на описании структурно-функциональных характеристик информационной системы и условий ее эксплуатации (организационно-технологической и пространственно-технической схемы), в рамках которых рассматриваются (моделируются) сценарии реализации известных УБИ.

В Методике-2021 рассматривается не конкретное определение или моделирование угроз, а их оценка (комплексная, экспертная и т. п.). Область применения методического документа разделена, как по видам информационных систем, так и по видам потенциальных угроз [7. С. 277–279]. Кроме того, отдельно выделены зоны ответственности для операторов и поставщиков услуг.

Особенностью документа является использование комплексного экспертно-аналитического подхода к процессам определения и моделирования УБИ. В Методике-2021 определено три этапа [5. С. 13–20]:

- I. Определение негативных последствий от реализации (возникновения) УБИ.
- II. Определение объектов воздействия УБИ.

III. Оценка возможности реализации (возникновения) УБИ и определение их актуальности.

В качестве исходных данных для определения возможных негативных последствий от реализации УБИ в информационной системе используются следующие источники [5. С. 35–42]:

- Приложение № 2 к Методике-2021 «Виды рисков (ущерба) и типовые негативные последствия от реализации УБИ»;
- Приложение № 4 к Методике-2021 «Рекомендации по формированию экспертной группы и проведению экспертной оценки при оценке угроз безопасности информации».

Оценка УБИ включает следующие этапы:

- определение негативных последствий, которые могут наступить от реализации (возникновения) УБИ;
- определение возможных объектов воздействия УБИ;
- оценка возможности реализации (возникновения) УБИ и определение их актуальности.

Оценка УБИ проводится с использованием экспертного метода опроса. Экспертную оценку рекомендуется проводить в отношении следующих параметров:

- негативного последствия от реализации УБИ;
- целей нарушителей по реализации УБИ;
- сценария действий нарушителей при реализации УБИ.

В Методике-2021 рекомендовано проводить оценку параметров опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты ответа в единой принятой шкале измерений.

Опрос экспертов, как правило, включает следующие этапы:

- каждый эксперт проводит оценку оцениваемого параметра, результаты которой заносятся в таблицу;
- после оценки каждым из экспертов отбрасываются минимальные и максимальные значения;
- определяется среднее значение оцениваемого параметра в каждом раунде;
- определяется итоговое среднее значение оцениваемого параметра.

Необходимо отметить, что, по словам регулятора, утвержденный алгоритм моделирования угроз разработан на основании лучших практик (Best Practices) и подразумевает два глобальных этапа: определение потенциальных угроз, которые возможны для информационной системы, исходя из ее исходных характеристик, и далее выявление актуальных угроз [7. С. 280–282].

При моделировании угроз по Методике-2021 можно использовать набор ТТР своего рода как примитивный конструктор на основе АТТ&СК. Имеется атака – формируются все пути ее реализации (сценарии) из «кубиков» ТТР, причем фреймворк MITRE АТТ&СК указывается как один из возможных источников для формирования исходных данных [10].

Таким образом, можно выделить некоторые особенности Методики-2021:

- документ имеет логически выстроенную структуру, содержит большое количество наглядных примеров и расширенный перечень источников;

– документ обладает универсальностью применения для информационных систем различного назначения;

– при построении моделей УБИ используются лучшие мировые практики, что делает эти модели более эффективными для защиты от актуальных угроз.

Недостатком является то, что действующий подход к моделированию УБИ делает процесс построения модели угроз сложным, требующим от исполнителя высокого уровня компетентности в сфере информационной безопасности, знания правовых основ и опыта работы в информационной системе. Сложность моделирования угроз подтверждается и тем, что ФСТЭК России конкретизировала типовые замечания по рассмотрению моделей УБИ [14. С. 4]:

1. Недостаточно определяются негативные последствия для видов ущерба, а также объекты воздействия.

2. Не в полной мере оцениваются виды нарушителей, которые могут реализовывать УБИ.

3. Внутренние пользователи (особенно ключевые сотрудники) часто не признаются актуальными нарушителями.

4. Не в полном объеме представлено описание сценариев реализации УБИ.

5. Недостаточно оценены УБИ, связанные с технологиями контейнеризации, виртуализации и облачного хранения данных.

Кроме того, наличие открытого доступа к подобной информации не обеспечивает ее эффективность, поскольку специалист по информационной безопасности пока вынужден «вручную» справляться с большим объемом данных.

Так, на середину 2022 г. БДУ ФСТЭК России содержит более 42 тыс. записей об уязвимостях и 222 записи об УБИ [1]. Указанная информация хранится в виде текстовых описаний, анализ которых требует существенных временных затрат и конкретных профессиональных навыков. Следовательно, актуальным на сегодня является вопрос использования методов семантического (интеллектуального) анализа текстов, методов NLP (обработки естественного языка), применение которых позволило бы решить в какой-то степени проблему автоматизации поиска и анализа конкретной информации в перечисленных выше источниках данных.

Таким образом, из возможных направлений исследований перспективным направлением может являться разработка методик автоматизированной оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования, методов машинного обучения и анализа данных с возможностью количественной оценки рисков нарушения кибербезопасности, расширяющей Методику-2021 [2. С. 115].

Кроме того, актуальным является вопрос как «взаимоувязать» (провести компаративный анализ) или интегрировать моделирование угроз по действующей методике ФСТЭК России и анализ по матрицам MITRE [6]. Профессиональное сообщество в дискуссионном контексте предлагает искать возможные варианты интеграции этих двух методик в следующих направлениях:

1. Выполнить анализ актуальных ТТР только по матрицам MITRE ATT&CK, а в модели угроз заменить их на наиболее подходящие техники и тактики из перечней ФСТЭК России.

2. Выполнить анализ изначально по Методике-2021, определить актуальные техники и тактики из перечней ФСТЭК России и провести корреляцию с техни-

ками и тактиками из матриц MITRE ATT&CK (тех, которых нет в действующей методике).

3. Выполнить анализ УБИ только по Методике-2021, но при выборе контрмер использовать имеющиеся у MITRE рекомендации по обнаружению и блокированию конкретных ТТР.

4. Принять во внимание маппинг техник MITRE ATT&CK в техники ФСТЭК в разрезе не техники нарушителей по Методике-2021 (их не так много и они не достаточно хорошо систематизированы и детализированы), а техники MITRE ATT&CK, которые не только лучше описаны, но и поддерживаются более широким сообществом специалистов, а на их базе построено не малое количество полезных в практической деятельности инструментов [6].

В заключении следует отметить, что действующий подход к моделированию угроз с возможностью интеграции рассмотренных выше методик станет эффективнее не только в стадии эксплуатации, но и на этапе создания систем защиты информации и будет более практико-ориентированным. Это улучшит способность противостоять УБИ, активно обнаруживать поведение злоумышленника и поддерживать надежный, контекстуальный двунаправленный обмен информацией.

Список литературы

1. Банк данных угроз безопасности информации // БДУ ФСТЭК России. URL: <https://bdu.fstec.ru/> (дата обращения: 27.06.2022).

2. Васильев В. И., Вульфен А. М., Кириллова А. Д., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. № 3. С. 110–134. DOI: 10.24412/2410-9916-2021-3-110-134

3. Макарова О. С., Поршнева С. В. Определение параметров, влияющих на возможность реализации компьютерной атаки нарушителем // Безопасность информационных технологий. URL: <https://bit.mephi.ru/index.php/bit/article/view/1336> (дата обращения: 27.06.2022). DOI: <http://dx.doi.org/10.26583/bit.2021.2.01>

4. Матрица ATT&CK. Как устроен язык описания угроз и как его используют // Hacker.ru. URL: <https://hacker.ru/2021/03/17/mitre-att-ck/> (дата обращения: 27.06.2022).

5. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 05.02.2021 // ФСТЭК России (Федеральная служба по техническому и экспортному контролю). URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhdn-fstek-rossii-5-fevralya-2021-g> (дата обращения: 27.06.2022).

6. Сайт Алексей Лукацкого «Бизнес без опасности». URL: <https://lukatsky.ru/mapping-attack-to-fstek> (дата обращения: 30.06.2022).

7. Суханов И. Д., Рыбкина О. В. Новые подходы к моделированию угроз безопасности информации // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке: труды Всероссийской научно-практической конференции творческой молодежи с международным участием (Хабаровск, 20–23 апреля 2021 г.). В 2 т. Т. 1 / под ред. А. Р. Едигаряна. Хабаровск: ДВГУПС, 2021. С. 277–282.

8. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утвержден ФСТЭК России 11.02.2013 № 17 // ФСТЭК России (Федеральная служба по техническому и экспортному контролю). URL: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17> (дата обращения: 29.06.2022).

9. Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка) // Собрание законодательства Российской Федерации. 2004. № 34. Ст. 3541; 2006, № 49, ст. 5192; 2008 № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, Ст. 818).

10. Что такое база знаний MITRE ATT&CK и зачем она нужна // Anomali. URL: <https://www.anomali.com/ru/resources/what-mitre-attck-is-and-how-it-is-useful> (дата обращения: 27.06.2022).

11. ATT&CK Matrix for Enterprise // MITRE ATT&CK®. URL: <https://attack.mitre.org/> (дата обращения: 27.06.2022).

12. MITRE // Mitre Corporation. URL: <https://www.mitre.org/focus-areas/cybersecurity> (дата обращения: 01.07.2022).

13. Best Practices for MITRE ATT&CK® Mapping // CISA is part of the Department of Homeland Security: [сайт]. – URL: <https://www.cisa.gov/uscert/best-practices-mitre-attckr-mapping> (дата обращения: 20.07.2022).

14. TB Forum Highlights & Market Insights // TB Forum Show Team, Groteck Business Media. URL: <https://www.tbforum.ru/blog/vo-vtoroj-den-tb-foruma-proshla-konferenciya-aktualnye-voprosy-zashchity-informacii> (дата обращения: 20.07.2022).

И. Д. Сулов,
магистрант,

Московский городской педагогический университет

СТАТУС ОНЛАЙН-ОБУЧЕНИЯ В СОВРЕМЕННОЙ СИСТЕМЕ ОБРАЗОВАНИЯ

Аннотация. В данной статье выявлены причины более широкого использования дистанционных технологий в образовательном процессе по программам дополнительного образования и повышения квалификации. Рассмотрен статус дистанционного обучения как правовой статус использования дистанционных образовательных технологий по программам среднего (основного, общего, профессионального) и высшего профессионального образования согласно законопроектам и приказам, предусматривающим изменение использования цифровых образовательных технологий по специальностям, использование верифицированных образовательных платформ и учебников.

Ключевые слова: образование, цифровая трансформация образования, дистанционное обучение, цифровизация, дистанционная образовательная технология, высшее профессиональное образование, дополнительное образование

THE STATUS OF ONLINE TEACHING IN THE MODERN EDUCATION SYSTEM

Abstract. This article identifies the reasons for the wider use of distance learning technologies in the educational process for additional education and advanced training programs. The status of distance learning is considered as the legal status of the use of distance learning technologies in secondary (basic, general, professional) and higher professional education programs according to draft laws and orders providing for changes in the use of digital educational technologies in specialties providing for full-time training and the use of verified educational platforms and textbooks.

Keywords: Education, Digital transformation of education, Distance learning, Digitalization, Distance education technology, Higher professional education, Additional education

Качество современного образования или образовательной услуги во многом зависит от ряда факторов, влияющих не только на процесс обучения, управления и контроля, но и на статус учебных заведений, форм обучения и уровень финансирования. За последние 10 лет система российского образования претерпела значительные изменения в области цифровой трансформации, что способствовало качественному улучшению уровня доступности образования. Появление новых форм обучения, связанных с использованием дистанционных технологий в учебном процессе, позволили существенно повысить уровень доступности образования, оптимизировать материальные и людские ресурсы. Поиск, сбор, агрегирование и анализ информации, необходимой для подготовки к уроку и разработки актуальных образовательных программ, в значительной степени сохраняют временные ресурсы и упрощают человеческую деятельность. Пик использования цифровых технологий в образовании приходился на 2020 г., период коронавирусной инфекции. В течение продолжительного времени учащиеся средних и высших образовательных учреждений обучались и сдавали экзамены дистанционно, что позволило беспрепятственно завершить обучение. Помимо профессиональных образовательных программ, взрослые и дети активно обучались по программам повышения квалификации или дополнительным онлайн – курсам по общеобразовательным предметам. Наряду с использованием дистанционных технологий, активно интегрировались в образовательный процесс образовательные продукты в виде приложений и онлайн – платформ от ведущих российских и зарубежных образовательных учреждений (Coursera, Skillbox, Открытое образование и т. д.).

В 2022 г. уровень использования дистанционных технологий в учебном процессе в средних и высших образовательных организациях значительно снизился по сравнению с 2020 г. В первую очередь это связано с изменениями ограничительных мер и поправок в области дистанционного обучения, в результате которых образовательные организации вернулись к очному формату обучения и использование цифровых технологий свелось к минимуму. Эти изменения не смогли в полной мере снизить уровень повсеместного использования средств дистанционного обучения. Так, например, представители сегмента образовательных услуг в лице организаций, осуществляющих обучение по программам дополнительного

образования и повышения квалификаций, продолжают массово использовать как средства дистанционного обучения, так и учебные приложения в образовательном процессе. Причиной столь массового применения цифровых технологий в данном сегменте рынка является перераспределение материальных, трудовых, временных и финансовых ресурсов с целью оптимизации деятельности организаций, осуществляющих предоставление данных образовательных услуг. Для таких организаций дистанционный формат обучения выгоден, поскольку не несет большие материальные затраты, позволяет значительно увеличить охват целой аудитории в масштабах региона, страны. Именно поэтому использование дистанционного формата обучения будет приоритетным для организаций, обучающих слушателей по программам дополнительного образования или повышения квалификации.

Статус дистанционного образования как формы обучения в образовательных организациях имеет весьма неоднозначную репутацию среди учащихся. Это вызвано рядом факторов:

- Новизна дистанционной формы обучения. Активное использование дистанционных технологий в российской системе образования пришлось на 2020 г. До этого дистанционный формат обучения не был столь массовым. Отсюда и возникает недоверие данной форме обучения со стороны участников образовательного процесса.

- Отсутствие объективных исследований об эффективности применения дистанционных технологий в средних и высших профессиональных образовательных учреждениях.

- Низкий статус образовательных организаций, обучающих по программам среднего и высшего образования в дистанционном формате.

- Недоверие со стороны работодателей к соискателям, обучившихся по программам среднего и высшего профессионального образования в дистанционном формате.

Существует значительное отличие в статусе между средним, высшим профессиональным образованием и дополнительным образованием, полученными в дистанционном формате. К получению дополнительного образования или повышению квалификации в дистанционном формате отношение со стороны людей более одобрительно. Это вызвано рядом следующих факторов:

- Организациями, осуществляющими предоставление образовательных услуг, являются известные российские компании: «Яндекс», «Сбер», «Ростелеком», Mail group и др. Высокий статус таких организаций обеспечивает доверие со стороны потенциальных потребителей и покупателей образовательных услуг.

- Совместные проекты государства с вышеперечисленными организациями для подготовки будущих ИТ – специалистов (Проект «Цифровые профессии» национального проекта «Цифровая экономика»).

- Наличие актуальных образовательных программ в сферах: ИТ, инженерия, управление, финансы, маркетинг, аналитика и т. п.

- Наличие актуальных образовательных продуктов: учебные приложения, образовательные платформы.

Таким образом, дистанционное образование по программам дополнительного образования и курсов повышения квалификации как сегмент рынка образования имеет достаточно высокий статус среди потребителей и покупателей образовательных услуг в сравнении с дистанционным обучением по программам среднего и высшего профессионального образования. Статус цифрового формата обучения будет расти среди людей пропорционально уровню развития сервиса, образовательных продуктов и образовательных программ.

Правовой статус дистанционного образования закреплён в Федеральном государственном образовательном стандарте. Так, Согласно Федеральному закону от 29.12.2012 № 273-ФЗ «Об образовании», где под электронным обучением понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. На основании вышеизложенного следует, что организации, использующие дистанционные формы обучения в образовательном процессе должны быть оснащены технологичным оборудованием, помещениями, серверами, и иными средствами для осуществления передачи информации. Иначе, организация не сможет в праве осуществлять образовательную деятельность в дистанционном формате. Мощности современных школ, университетов и колледжей позволяют использовать дистанционные формы обучения в образовательной деятельности. Это обусловлено рядом как федеральных, так и национальных программ, направленных на цифровизацию общества, в том числе и системы образования. Организации, осуществляющие предоставление образовательных услуг по программам дополнительного образования и курсов повышения квалификации, не всегда имеют достаточное количество мощностей для осуществления своей деятельности. Исключения составляют организации-гиганты («Сбер», «Яндекс», «Ростелеком» и др.).

Под дистанционными образовательными технологиями понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников. Согласно ст. 16 ч. 2 организации, осуществляющие образовательную деятельность вправе применять дистанционные образовательные технологии при реализации образовательных программ в порядке, установленном Правительством Российской Федерации. Получение профессий и специальностей среднего профессионального образования обуславливается перечнем образовательных программ, по которым не допускается электронное обучение ввиду специфики получаемой специальности обучающимися. Перечень специальностей и направлений подготовки высшего образования, реализация образовательных программ по которым не допускается с применением исключительно электронного обучения, дистанционных образовательных технологий, утверждается федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому

регулированию в сфере высшего образования. Именно поэтому в высших и средних профессиональных образовательных организациях отсутствует обучение по специальностям, не предусматривающим обучение с использованием дистанционных форм. Организации, осуществляющие подготовку по программам дополнительного образования и курсов повышения квалификации, повсеместно используют в своей образовательной деятельности цифровые технологии. Аналогично со средним и высшим профессиональным образованием в дополнительном образовании разрешено обучать лишь по тем специальностям, в учебных программах которых предусмотрено использование дистанционных технологий.

Согласно Федеральному закону от 26.05.2021 № 144-ФЗ. О внесении изменений в Федеральный закон «Об образовании в Российской Федерации», с 1 сентября 2023 г. организации, осуществляющие образовательную деятельность и имеющие государственную аккредитацию по образовательным программам среднего профессионального образования, реализуемым на базе основного общего образования или интегрированным с образовательными программами основного общего и среднего общего образования, при освоении учебных предметов, курсов, дисциплин основного и (или) среднего общего образования обязаны использовать верифицированные онлайн – платформы, учебники и электронные образовательные ресурсы, входящие в соответствующий федеральный перечень. Высшее профессиональное образование данные изменения не затрагивают. Данная унификация позволит существенно улучшить качество образовательных платформ и учебных пособий. Тем самым, статус цифровых образовательных ресурсов и их использование в обучении будет непрерывно расти.

С 1 сентября 2023 г. ограничивается использование дистанционных образовательных технологий, электронного обучения в образовательном процессе организациями Приказом Минобрнауки России № 465, Минпросвещения России № 345 от 19.05.2022 Согласно законопроекту № 159399-8 «О внесении изменений в Федеральный закон «Об образовании Российской Федерации», использование дистанционных технологий в очной форме обучения предусматривается только в отношении обучающихся, подлежащих ограничительным мероприятиям (карантину) и случаев, когда применение дистанционных образовательных технологий допускается при осуществлении обучения по очной форме. Образовательные организации вернулись к очному формату обучения, и использование цифровых технологий свелось к минимуму. В связи с этим появился смешанный формат обучения, где отсутствует подробное отличие между очной, очно – заочной и заочной формы обучения. Субъекты права законодательной инициативы считают, что взаимодействие обучающихся и педагогических работников в основном заменяется их опосредованным (на расстоянии) взаимодействием с применением информационно – телекоммуникационных сетей. Фактически, происходит подмена очной формы обучения очно-заочной или даже заочной.

Развитие технологий в области цифровой передачи информации в будущем может позволить сократить перечень специальностей, обучение по которым в дистанционном формате не предусмотрено учебной программой. Правовой статус дистанционного образования еще не раз будет изменяться, и аналогично изменению правового

статуса будет меняться отношение общества к технологиям дистанционного обучения. Мы предполагаем, что существенное развитие данная форма обучения получит в дополнительном образовании, поскольку последние законопроекты сильно не ограничивают данную структуру системы образования в использовании цифрового обучения. Это приведет к созданию новых цифровых образовательных продуктов, развитию методики обучения в условиях цифровой трансформации общества и открытию иных направлений образования, в том числе и новых форм обучения.

Список литературы

1. Голышев В. Г., Голышева А. В. К вопросу о некоторых организационно-правовых аспектах дистанционного образования в высшей школе // Новые технологии оценки качества образования: сб. мат. XVI Форума Гильдии экспертов в сфере профессионального образования в рамках онлайн-конференций. Москва, 2021. С. 15–19.

2. Приказ Министерства науки и высшего образования Российской Федерации, Министерства просвещения Российской Федерации от 17.06.2022 «О признании утратившим силу приказа Министерства образования и науки Российской Федерации от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ» // СПС «КонсультантПлюс».

3. Федеральный закон от 26.05.2021 № 144-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» // СПС «КонсультантПлюс».

4. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» // СПС «КонсультантПлюс».

И. О. Ташбаев,

PhD, член Международного союза экономистов ООН, академик,
Международная академия менеджмента, доцент,
Ташкентский государственный аграрный университет

Э. Омонкулов,

бакалавр

ЦИФРОВАЯ ЭКОНОМИКА – ВАЖНЫЙ ФАКТОР РАЗВИТИЯ НОВОГО УЗБЕКИСТАНА

Аннотация. В статье затрагивается тема цифровой экономики как важного фактора развития нового Узбекистана. Республика Узбекистан является крупной страной с развитой экономикой среди стран Центральной Азии. Узбекистан показан как организатор и регулятор технологических реформ, который систематически совершенствует свою нормативную базу, регулируя развитие цифровизации экономики, мотивирует внедрение в ИКТ, способствует подготовке необходимых специалистов по IT-технологии, защите от киберугроз, организует сотрудничество с развитыми странами по IT-технологиям.

Ключевые слова: цифровая экономика, цифровая трансформация, экспортный потенциал, природные ресурсы, высокоскоростной Интернет, единый портал интерактивных и реестр электронных государственных услуг, IT-технологии, IT-парк

DIGITAL ECONOMY IS AN IMPORTANT FACTOR IN THE DEVELOPMENT OF THE NEW UZBEKISTAN

Abstract. The article deals with the topic of digital economy as an important factor in the development of the new Uzbekistan. The Republic of Uzbekistan is a large country with a developed economy among Central Asian countries. Uzbekistan is shown as an organizer and regulator of technological reforms, which systematically improves its regulatory framework, regulating the development of the digitalization of the economy, motivates the introduction of ICT, promotes the training of necessary specialists in IT technology, protection from cyber threats, organizes cooperation with developed countries on IT technologies.

Keywords: Digital economy, Digital transformation, GDP growth, Natural resources, High-speed Internet, a single interactive portal and register of electronic government services, IT technologies, IT park

Узбекистан является страной с крупной экономикой в Центральной Азии (далее – ЦА) с объемом ВВП 69,2 млрд долл., населением 35,6 млн человек (в 2022 г.). Страна богата природными ресурсами и обладает развитой производственной базой. Рост потенциального ВВП Узбекистана составляет около 5,5 % в год. Золотовалютные резервы Узбекистана на 1 мая 2022 г. составили 35,9 млрд долл.

Агропромышленный комплекс – стратегическая для Узбекистана отрасль, имеющая высокий экспортный потенциал в продуктах сельского хозяйства. Перед республикой стоит амбициозная задача – увеличить в два раза объем экспорта продукции агропромышленного комплекса. Экспортный потенциал агропромышленного комплекса оценивается более чем в 5 млрд долларов США в год. Без цифровизации агропромышленного комплекса и резкого повышения эффективности предприятий сельскохозяйственных продуктов обеспечить такой рост невозможно. Для воплощения в жизнь АПК цифровой трансформации требуются специалисты, обладающие новыми знаниями и умениями в области IT-технологии.

Опыт стран всего мира показывает, что цифровая экономика развивается и должна основываться на инновационных решениях. В настоящее время в Республике Узбекистан непрерывно ведутся работы по подключению всех городов и районных центров к сетям высокоскоростного Интернета. В нашей республике по этому перспективному направлению работа началась с принятием Закона Республики Узбекистан ЗРУ-395 от 09.12.2015 «Об электронном правительстве», в котором основными задачами обозначены необходимость обеспечения эффективности, оперативности и прозрачности деятельности государственных органов, усиления их ответственности и исполнительской дисциплины, создание дополнительных механизмов обеспечения обратной связи с населением и субъектами предпринимательства [1]. Согласно данному Закону, на всей территории страны создаются возможности для заявителей по осуществлению взаимоотношений

с государственными органами в рамках электронного правительства. Формируются базы данных государственных органов в рамках возложенных на них функций, Единого портала интерактивных государственных услуг и Единого реестра электронных государственных услуг. В систему государственного управления внедрен принцип единого окна при осуществлении взаимоотношений с населением и субъектами предпринимательства за счет формирования механизмов электронного документооборота, взаимодействия и обмена информацией между базами данных государственных органов. Осуществлена работа по переводу субъектов предпринимательства на использование электронного документооборота, статистической отчетности, таможенного оформления, выдачи лицензий, разрешений, сертификатов, а также получения информации от государственных органов. Кроме того, расширяется использование субъектами предпринимательства систем электронной коммерции, сбыта продукции и осуществления закупок через всемирную информационную сеть Интернет, а также внедряются автоматизированные системы учета, контроля и оплаты коммунальных услуг и развиваются системы безналичных электронных платежей, осуществления государственных закупок, дистанционного доступа и других электронных форм деятельности в банковско-финансовой сфере. В них отражены приоритетные направления развития инфраструктуры информационно-коммуникационных технологий (ИКТ), реформирования государственного управления и оптимизации государственных услуг, обеспечения информационной безопасности «электронного правительства».

Стратегия действий по дальнейшему развитию Республики Узбекистан в 2017–2021 гг. предусматривала основные направления поступательного движения страны в перспективе [2]. Целью Стратегии действий являлось коренное повышение эффективности проведенных реформ, создание условий для обеспечения всестороннего и ускоренного развития государства и общества, модернизация страны и либерализация всех сфер жизни.

Начата реализация свыше 220 приоритетных проектов, предусматривающих совершенствование системы «электронного правительства», дальнейшее развитие отечественного рынка программных продуктов и информационных технологий, организацию во всех регионах республики IT-парков, обеспечение данной сферы квалифицированными кадрами [3].

В результате реализации концепции были созданы удобства населению и бизнесу в получении государственных услуг, улучшены условия ведения бизнеса, ведутся работы по оптимизации численности госслужащих, увеличению рабочих мест за счет внедрения новых услуг, которые предоставляют возможность для вхождения республики в число ведущих стран мира по уровню развития «электронного правительства» и по уровню обеспечения кибербезопасности. Однако это очень сложная задача, предлагаем поразмыслить над тем, что нас ожидает от внедрения цифровой экономики с целью интеграции в мировую экономику, приводим цитаты из доклада цифровой экономики еще в 2019 г., UNCTAD [4]. Без принятия соответствующих мер огромный разрыв между странами со слабым развитием интернет-связи и странами с весьма высоким уровнем цифровизации будет лишь увеличиваться так же,

как и существующее неравенство. Цифровой разрыв, различная степень готовности стран и высокая концентрация рыночного влияния в цифровой экономике указывают на необходимость принятия новых стратегий и регулирующих положений, способствующих более справедливому распределению выгод от происходящего процесса преобразований под влиянием цифровых технологий. Осуществление этого представляется сложной задачей.

Цифровизация по-разному сказывается на отдельных странах, и правительствам требуется пространство для маневра в своих действиях, с тем чтобы регулировать цифровую экономику в интересах достижения широкого круга обоснованных целей государственной политики. Управление цифровыми данными и их регулирование являются трудной задачей, поскольку затрагивают такие сферы, как права человека, торговля, создание экономической стоимости и получение выгод, соблюдение законодательства и обеспечение национальной безопасности. Разработать политику, которая бы учитывала все эти разнообразные аспекты, довольно сложно, однако без этого не обойтись. Кроме того, чтобы обеспечить эффективное распределение выгод и устранить негативные последствия цифровизации, потребуются дополнительные меры социальной защиты, а также более активные усилия, направленные на переподготовку работников [3]. Поиск подходящих решений требует более широкого международного сотрудничества и проведения диалога по ключевым вопросам при всестороннем участии развивающихся стран. Учитывая сложность и новизну рассматриваемых вопросов, а также неизменно быстрые темпы технологического процесса, необходимо будет проверить на практике различные возможные стратегии, с тем чтобы оценить их преимущества и недостатки. Сегодня высокоскоростной доступ к Интернету имеют более тысячи учреждений здравоохранения, дошкольного и школьного образования [5].

Таким образом, необходимо отметить, что перед государством стоят очень сложные задачи по внедрению цифровой экономики в жизнь, и эти работы требуют больших инвестиций, но без цифровизации экономики не будет в целом экономического развития сегодня и в будущем, так как это требование жизни. Цифровизация экономики позволит стране в кратчайшие сроки решить вопрос глобальной конкурентоспособности и национальной безопасности. «Цифровая экономика» – это обеспечение цифрового пространства для всех сфер жизнедеятельности страны. В Постановлении Президента от 28.04.2020 предусмотрены меры по широкому внедрению IT-технологий в госуправление, производство, сельское хозяйство и социальную сферу. Текущее состояние цифровой трансформации в республике составляет 700 информационных систем, 30 % из них подключены к «электронному правительству». Инновационный потенциал сельского хозяйства имеется в электронной системе учета земли и воды, а также цифровизации методов выращивания сельскохозяйственных культур. Ожидаемый рост ВВП при 10 %-м расширении сетей скоростного Интернета составляет 1 %, а также повышение урожайности за счет четкого определения агротехнических мероприятий составляет 25–30 % [6].

Опыт стран всего мира подтверждает эффективность цифровой экономики.

В последних выступлениях Президент Республики Узбекистан неоднократно отмечал: «Главы регионов и отраслей обязаны осознать, что без цифровизации не

будет результата, не будет развития. Каждый год промедления может отбросить страну в развитии на десятилетия». В Постановлении Президента № 4699 от 28.04.2020 предусмотрены меры по широкому внедрению ИТ-технологий в сферу государственного управления, производство, энергетику, сельское хозяйство и социальную сферу.

Указом Президента от 05.10.2020 № УП-6079 утверждена Стратегия «Цифровой Узбекистан – 2030». Руководители всех уровней должны определить этот вопрос как свою повседневную задачу, глубоко изучить сферу цифровизации с самых азов. Принято Постановление Правительства от 17.12.2020 № 794 «О мерах по развитию системы цифровизации в агропромышленном комплексе и сельском хозяйстве Республики Узбекистан».

В 2022 г. запускается «Единая агроплатформа в агропромышленном комплексе» для цифрового взаимодействия фермеров и агрокластеров с поставщиками и обслуживающими организациями.

В 2022–2023 гг. планируется запустить еще пять информационных систем, призванных упростить предпринимательскую деятельность а АПК облегчить обращения юридических и физических лиц в государственные органы, получать интерактивные услуги.

Постановлением создано государственное учреждение «Центр цифровизации агропромышленности» при Министерстве сельского хозяйства. До 1 мая 2021 г. реализован экспериментальный проект по автоматизации крупных гидроузлов и ирригационных систем на основе цифровых технологий. Утвержден Адресный перечень по внедрению технологий «Умного сельского хозяйства» в регионах республики.

Ежемесячно растет количество абонентов мобильной связи. По состоянию на 01.04.2022 оно достигло 29,9 млн человек, а интернет-пользователей – 27,2 млн человек.

Если проанализировать рост объема оказанных услуг по виду экономической деятельности сферы «Информатизация и связь», то он составил 12,9 трлн сум, при этом темп роста составил 115,3 %.

Цифровизация экономики позволит стране в кратчайшие сроки решить вопрос глобальной конкурентоспособности и национальной безопасности. Перед государством стоят сложные задачи по ускорению внедрения цифровой экономики в жизнь, и эти работы требуют больших инвестиций.

Если посмотреть динамику развития телекоммуникационной инфраструктуры, общая протяженность волоконно-оптических линий связи составила 118 тыс. километров, а число базовых станций мобильной связи – более 46 тыс. единиц.

Цифровизация создает пространство для маневра. Сохраняя стабильные темпы роста, к 2030 г. планируется достичь ВВП на душу населения, равный 4000 долл. США, и таким образом войти в категорию «государств с доходом выше среднего» и развить цифровую экономику с увеличением ее доли не менее чем в 2,5 раза к концу 2026 г.

Государство как организатор и регулятор технологических реформ систематически совершенствует нормативную базу, регулируя развитие цифровизации экономики, мотивирует внедрение в ИКТ, способствует подготовке необходимых специалистов по ИТ-технологии, защите от киберугроз, организует сотрудничество с развитыми странами по ИТ-технологиям.

В рамках проводимых реформ, а также Стратегии развития нового Узбекистана на 2022–2026 гг., утвержденной Указом Президента Республики Узбекистан от 28.01.2022 № 60, особое внимание уделяется цифровизации основных сфер деятельности и построению в стране подлинного информационного общества [7]. Инвестиции в цифровую экосистему, IT-инфраструктуру и электронные услуги будут способствовать дальнейшей модернизации нашей экономики во всех сферах.

Выводы. Для полного воплощения и развития государство должно выступать как организатор и регулятор технологических реформ; систематически совершенствовать нормативную базу, регулируя развитие цифровизации экономики; мотивировать внедрение в организациях ИКТ; в краткие сроки подготовить необходимых специалистов по IT-технологии; быть созидателем безопасности от киберугроз; организовать сотрудничество с развитыми странами по IT-технологии; ускоренно внедрять инновационные IT-технологии повсеместно, включая агропромышленный комплекс республики.

Цифровизация сельского хозяйства занимает одну из лидирующих позиций, так как от степени развития сельскохозяйственной отрасли в стране во многом зависит экономическая стабильность государства. Сельское хозяйство в мире превращается из традиционной в высокотехнологичную отрасль, которая способна создать новые рынки для инновационных решений и разработок.

Список литературы

1. Закон Республики Узбекистан № ЗРУ-395 от 09.12.2015 «Об электронном правительстве».
2. Указ Президента Республики Узбекистан от 07.02.17 № УП-4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан».
3. Указ Президента Республики Узбекистан от 05.10.2020 № УП-6079 «Об утверждении стратегии “Цифровой Узбекистан – 2030” и мерах по ее эффективной реализации».
4. Что такое цифровая экономика? Тренды, компетенции, измерение: докл. к XX Апр. междунар. науч. конф. по проблемам развития экономики и общества. Москва, 9–12 апр. 2019 г. / Г. И. Абдрахманова, К. О. Вишнеvский, Л. М. Гохберг и др. Москва: Изд. ВШЭ, 2019. 82 с.
5. Указ Президента Республики Узбекистан от 02.03.2020 «О Государственной программе по реализации Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017–2021 годах в Год развития науки, просвещения и цифровой экономики».
6. URL: <https://uz.sputniknews.ru/20200922/V-Uzbekistane-vnedryat-tsifrovuyu-ekonomiku-i-elektronnoe-pravitelstvo-15032608.html>
7. Указ Президента Республики Узбекистан от 28.01.2022 № УП-60 «О Стратегии развития нового Узбекистана на 2022–2026 годы».

А. И. Трахов,

доктор юридических наук, профессор,
Кубанский государственный университет

З. М. Бешукова,

доктор юридических наук, доцент,
Адыгейский государственный университет

ПРЕДУПРЕЖДЕНИЕ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА: РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ

Аннотация. Исследование опыта Российской Федерации по предупреждению телефонного мошенничества показало, что повышение уровня осведомленности населения об особенностях мошеннических схем, о функционировании тех или иных финансовых механизмов является очень важным направлением. Однако, как показывает практика, одних знаний для эффективного противодействия обозначенному виду преступлений явно недостаточно. Необходимо выработать у населения навыки безопасного поведения в различных ситуациях. Исследование относимого опыта Канады показало, что комплекс мер по предупреждению телефонного мошенничества в Российской Федерации и Канаде имеет много общих черт по своему содержанию, но отличается в части его организационной составляющей.

Ключевые слова: мошенничество, телефонное мошенничество, предупреждение, профилактика, зарубежный опыт, виктимность, комплексный подход

TELEPHONE FRAUD PREVENTION: RUSSIAN AND FOREIGN EXPERIENCE

Abstract. A study of the experience of the Russian Federation in the prevention of telephone fraud has shown that raising the level of public awareness about the features of fraudulent schemes, about the functioning of certain financial mechanisms is a very important area. However, as practice shows, knowledge alone is clearly not enough to effectively counter the designated type of crime. It is necessary to develop among the population the skills of safe behavior in various situations. A study of the comparable experience of Canada showed that the set of measures to prevent telephone fraud in the Russian Federation and Canada has many similarities in content, but differs in terms of organizational component.

Keywords: Fraud, Telephone fraud, Warning, Prevention, Foreign experience, Victimization, Integrated approach

Введение. Главным и неотъемлемым атрибутом современного мира является интенсивное развитие цифровых технологий. Сегодня люди в большинстве стран мира воспринимают беспилотные автомобили, бытовые роботы, денежные переводы по одному клику, умные дома и так далее как вполне нормальное, само собой разумеющееся явление. Цифровые технологии обновляются со стремительной скоростью. Однако с такой же скоростью развивается и киберпреступность, которая несет в себе угрозы, которые во многих случаях сложно, а иногда и невозможно,

сопоставить с преступлениями, совершаемыми в реальном (физическом) мире. Еще один важный аспект заключается в серьезной трансформации киберпреступности: из акций одиноких компьютерных гениев, она превратилась в хорошо организованный сверхприбыльный теневой бизнес.

Наглядно сказанное выше можно продемонстрировать на потерях банков и их клиентов в результате киберпреступлений. Так, в 2018 г. преступники взломали системы индийского Cosmos Bank и вывели в общей сложности почти 944 млн рупий (13,5 млн долл.). Причем, из них 805 млн рупий были похищены в течение 2 часов путем 14849 транзакций, осуществленных в 28 странах мира (!). Сумму в размере 139 млн рупий преступники перевели на счет гонконгской компании, выполнив 3 несанкционированные транзакции через глобальную платежную сеть SWIFT [4].

Однако все же самой популярной формой хищений чужого имущества в виртуальном пространстве является телефонное мошенничество. Именно оно с каждым днем набирает все большие обороты и превращается в настоящую пандемию. Ежегодные совокупные потери от телефонного мошенничества достигли астрономических цифр. Если говорить об ущербе от этого вида преступлений в Российской Федерации, то, по данным Банка России, в первом квартале 2022 г. граждане совершили более 258 тыс. переводов мошенникам на общую сумму почти 3,3 млрд рублей. При этом за аналогичный период в 2021 г. было зафиксировано 237,7 тысячи подобных случаев, сумма ущерба составила около 2,8 млрд рублей [1]. Полагаем, что названные суммы являются лишь приблизительными. Точно подсчитать, конечно, невозможно, поскольку телефонное мошенничество имеет высокую степень латентности.

Необходимо отметить, что телефонное мошенничество – это проблема не отдельно взятого государства, оно представляет угрозу для многих стран. И, соответственно, вопросы предупреждения и профилактики данного вида мошенничества включены в актуальную повестку дня современных государств.

Основная часть. В настоящее время наиболее популярные мошеннические схемы во многих государствах мало чем отличаются друг от друга. Телефонное мошенничество осуществляется посредством телефонных звонков от реальных людей, текстовых сообщений или автоматических звонков. Все звонки и текстовые сообщения, в зависимости от тех эмоций и чувств, которые они вызывают у потенциальной жертвы, можно разделить на 3 группы:

1) содержащие для жертвы хорошие новости (например, возможность купить тот или иной товар дешевле его рыночной стоимости; инвестировать свои деньги или получить бесплатные пробные версии продуктов; получить компенсацию за ранее приобретенные биологически активные добавки; снизить процентную ставку по ипотечному кредиту; выигрыш в лотерее и др.),

2) содержащие для жертвы плохие новости (например, угрозы уголовным наказанием за просмотр сайта с незаконным контентом; просьба о помощи от близкого родственника; сообщение от службы безопасности банка о подтверждении транзакции либо о подозрительной активности на банковском счете и др.),

3) содержащие для жертвы нейтральные новости (например, поучаствовать в благотворительной акции; получить доступ к SMS и звонкам другого человека; спасти бездомных животных и др.).

Безусловно, преступники постоянно актуализируют свои схемы, однако практически все их кампании построены примерно по одному алгоритму. Следует отметить, что легкодоступные инструменты для выполнения спуфинга позволяют идентифицировать номер входящего звонка как подлинный государственный или корпоративный номер. Последнее в свою очередь объясняет, почему в ряде зарубежных государств наиболее востребованными среди мошенников стали схемы со звонками от якобы представителей государственных органов. Именно виртуозное использование последних достижений в сфере высоких технологий в купе с отличным владением навыками коммуникации и в достаточной степени знаниями в области психологии (вхождение в доверие, использование способов манипулятивного воздействия на психику и т. д.) позволяет мошенникам достигать свои преступные цели. Жертвой мошеннических действий может стать абсолютно любой. И, если в предыдущие годы жертвами чаще других становились пожилые люди, то в последние годы возрастные рамки среди потерпевших практически стерлись. Все чаще и чаще жертвами мошенников становятся молодые технически «подкованные» люди.

Важной составляющей противодействия любому виду преступлений является профилактика. В свою очередь, в соответствии со ст. 6 Федерального закона от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», одним из основных направлений профилактики правонарушений является повышение уровня правовой грамотности и развитие правосознания граждан. К наиболее эффективным мерам по профилактике любого вида мошенничества относится рост интереса к этой теме со стороны общественности. Именно большое внимание общественности к различным мошенническим схемам значительно сокращает срок жизни даже самых хитрых сценариев, а из нетипичных они все быстро превращаются в типовые. Лучший способ избежать уловок телефонных мошенников – это осведомленность о том, какие схемы существуют. Министерство внутренних дел Российской Федерации проводит серьезную работу в этом направлении, в том числе и с привлечением общественности. В числе составляющих этой работы можно назвать проведение акций по распространению среди населения памяток по профилактике различных видов мошенничества; производство видеороликов, содержащих важные советы о том, как не стать жертвой мошенников и последующее их распространение, в том числе посредством различных мессенджеров и в социальных сетях и др.

Необходимо отметить также и то, что в Российской Федерации противодействие телефонному мошенничеству осуществляется по различным направлениям не только со стороны органов государственной власти, но и со стороны банков, иных финансовых структур и операторов телефонной связи. В частности, многие банки и операторы телефонной связи разработали и запустили комплексные программы по противодействию мобильному мошенничеству, включающие целый ряд мер. Тем не менее следует согласиться с мнением, что «для различных организаций характерны разные подходы к вопросам управления рисками, связанными с мошенничеством, а также разная степень интенсивности соответствующих мер» [2. С. 148].

Данные официальной статистики о количестве зарегистрированных преступлений, связанных с хищениями с использованием информационных технологий, позволяют утверждать, что, несмотря на принимаемые меры по осведомленности

граждан о фактах мошенничества и его различных схемах, мошенничество, в том числе и телефонное, по-прежнему представляет серьезную угрозу. И, конечно, возникает вопрос: почему люди верят мошенникам, и какие меры необходимо еще предпринять в целях профилактики совершения подобных преступлений?

Несомненно, роль повышения уровня осведомленности населения об особенностях мошеннических схем, о функционировании тех или иных финансовых механизмов, как и финансовой грамотности в целом, неоспорима. Безусловно, работу в этом направлении необходимо продолжать. Однако для того, чтобы люди перестали верить мошенникам даже широчайшего информирования недостаточно. Одних знаний, как показывает практика, явно мало. Необходимо выработать у населения навыки безопасного поведения в различных ситуациях. Полагаем, что именно такая новая задача должна быть поставлена перед всеми субъектами профилактики правонарушений.

В контексте сказанного вызывает научный интерес соответствующий зарубежный опыт. В Канаде значительный вклад в противодействие телефонному мошенничеству вносит Бюро по вопросам конкуренции (Competition Bureau Canada) – независимый правоохранительный орган, который защищает и продвигает конкуренцию в интересах канадских потребителей и предприятий [3]. Бюро по вопросам конкуренции, наряду с Королевской канадской конной полицией и Канадским центром по борьбе с мошенничеством, является одним из сопредседателей Форума по предотвращению мошенничества (The Fraud Prevention Forum). В настоящее время Форум объединяет более 60 организаций, члены которых работают над тем, чтобы канадцы не становились жертвами мошенничества, обучая их тому, как распознавать и противостоять фактам мошенничества, а также сообщить о них. В марте каждого года Форум проводит кампанию «Месяц по предотвращению мошенничества», направленную на повышение осведомленности о мошенничестве [3].

Следует отметить, что, несмотря на то, что банки и другие финансовые организации Канады продолжают совершенствовать технологии и способы борьбы с мошенничеством, потребители и предприятия принимают активное участие в защите самих себя. В течение всего марта Бюро по вопросам конкуренции и его партнеры по Форуму по предотвращению мошенничества участвуют в различных мероприятиях, направленных на информирование канадцев о последствиях мошенничества и о том, как защитить себя [3]. Кроме того, на официальном сайте Бюро по вопросам конкуренции имеется специальный раздел по предотвращению мошенничества. В данном разделе содержится подраздел «Проверьте свои знания о мошенничестве», при переходе в который предлагается пройти тестирование. Анализ представленных вопросов позволяет сделать вывод, что по большей части это ситуационный тест, т. е. вопросы построены по следующему принципу: для каждого предложенного сценария тестируемому предлагается 3–4 варианта действий, из которых он выбирает один или несколько, по его мнению, верных. Особый интерес для настоящего исследования представляет именно этот подраздел, поскольку ситуационные тесты позволяют не просто осуществлять контроль знаний, но и в определенной степени способствуют формированию навыков применения полученных знаний на практике, о необходимости наличия которых нами было сказано выше. Приведем пример вопроса и предложенных вариантов ответа:

Вы получаете тревожный звонок от человека, который представляется представителем органов государственной власти. Он утверждает, что недавняя проверка вашего счета показала, что вы должны деньги и что вы должны немедленно заплатить. Что вы сделаете, чтобы проверить это утверждение?

А. Вы даете звонящему свою контактную информацию и сообщаете, что не будете отправлять деньги, пока не получите копию удостоверения личности звонящего по электронной почте или факсу.

В. Вы кладете трубку и звоните по официальному номеру телефона государственного учреждения, представителем которого якобы является звонивший, и спрашиваете о состоянии вашего счета.

С. Вы платите требуемую сумму и настаиваете на том, чтобы впоследствии вам была отправлена квитанция или письмо-подтверждение. [3].

Кроме того, тестирование включает и типовые вопросы, например:

2. Кто обычно становится жертвой мошенников?

А. Пожилые люди.

В. Приезжие в Канаде.

С. Женщины старше 50 лет.

Д. Каждый. [3].

Следует отметить, что в Российской Федерации подобного рода тестирование предлагается пройти на сайтах различных банков.

Заключение. Аккумулируя все ранее изложенное, можно сделать вывод, что комплекс мер по предупреждению телефонного мошенничества в Российской Федерации и Канаде имеет много общих черт по своему содержанию, но отличается в части организационной составляющей. Полагаем, что в целях эффективного противодействия телефонному мошенничеству целесообразно дополнительно проработать вопрос консолидации и координации усилий органов государственной власти, общественности, финансовых организаций, бизнес-структур, институтов гражданского общества и т. д. по предупреждению преступлений, связанных с хищениями с использованием информационных технологий.

Список литературы

1. Загайнов М. ЦБ предложил новые меры по защите жертв мошенников // Российская газета. 2022. 11 августа.

2. Камко А. С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей: дисс. ... канд. юрид. наук. Владивосток, 2020. – 228 с.

3. Competition Bureau Canada. – URL: <https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/home> (дата обращения: 14.09.2022).

4. Rajendra Jadhav. Cosmos Bank loses \$ 13.5 million in cyber attack. – 2018. – August. – URL: <https://www.reuters.com/article/cyber-heist-india-idINKBN1KZ1J9> (дата обращения: 14.09.2022).

Ю. А. Трусов,

кандидат политических наук, ведущий советник,
Министерство науки и высшего образования Российской Федерации

А. В. Антипов,

кандидат философских наук, младший научный сотрудник,
Институт философии Российской академии наук

ПРАВО НА ЗАБВЕНИЕ: ОПЫТ ПРАКТИЧЕСКОГО АНАЛИЗА

Аннотация. Современный мир все более наполняется сервисами, которые делают нашу повседневность проще. Но простота оборачивается необходимостью иметь дело с тем, что по мере использования человек как сознательно (выкладывая пост в соцсети), так и нет (заходя на сайт и соглашаясь с политикой конфиденциальности) оставляет большое количество данных, которые используются в разных целях. Некоторая часть этой информации может носить приватный характер. Поэтому ее раскрытие для третьих лиц расценивается как нежелательное, а для возможности сохранения приватности вводится право на забвение. На кейсах утечек данных показывается, что право на забвение потенциально способно решить часть возникающих затруднений, определить и элиминировать риски технологического развития.

Ключевые слова: право на забвение, приватность, политика данных, утечка данных, безопасность, Интернет, конфиденциальность

RIGHT, TO BE FORGOTTEN: THE EXPERIENCE OF THE PRACTICAL ANALYSIS

Abstract. The modern world is increasingly filled with services that make people's lives easier. But simplicity turns into the fact that people knowingly (by posting on social networks) or not (by accessing the site and agreeing to the privacy policy) leave a large amount of data on the Internet that is used for various purposes. Some of this information is private. Therefore, its disclosure to third parties is regarded as undesirable, and for the possibility of maintaining privacy, the right to be forgotten is introduced. Case studies of data leaks show that the right to be forgotten can potentially solve some of the difficulties that arise, reducing the risks of technological development.

Keywords: Right, to be Forgotten, Privacy, Data Policy, Data Leaks, Safety, Internet, Confidentiality

I. Право на забвение в законодательстве. На данный момент право на забвение стало не просто философским понятием, но и юридически закрепленным термином, присутствующим в европейском законодательстве. Оно стало результатом длительной работы европейских институтов.

Важную роль в возникновении права на забвение в Европе сыграло знаменательное дело Марио Костехи Гонзалеса (Mario Costeja González) против Google Spaine. В конце 90-х у Марио возникли проблемы с имуществом из-за долга. В 1998 г. об этом инциденте написала местная газета, а позже оцифрованная версия была выложена в Интернет. Неприятный случай с долгом был разрешен, но проблема возникла с поисковым запросом. Поисковая система Google на запрос

ФИО Гонзалеса выводила данные о долговых проблемах, что сказывалось на его репутации. Он попытался удалить информацию как из газеты, так и из выдачи Гугл, так как эта информация уже не актуальна, но получил отказ. И вот в 2014 г. суд ЕС постановил, что поисковая система обязана при необходимости исправлять результаты поиска по запросу граждан. Этот прецедент открыл путь праву на забвение в Европе.

В 2016 г. вместо устаревшей Директивы 95/46/ЕС принимают Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС. Статья 17 впервые закрепляет такое понятие, как «право на забвение». С другой стороны, данный документ сводит право на забвение к праву на удаление (right to erasure), которые в рамках данного документа означают одно и то же. «Субъект данных имеет право требовать от контролера незамедлительного удаления относящихся к нему персональных данных, контролер должен незамедлительно удалить персональные данные» [2] при определенных условиях: персональные данные больше нет нужды обрабатывать, субъект отзывает согласие на обработку данных, субъект возражает против обработки или персональные данные собирались незаконно.

Естественно, право на забвение ограничивается в целях соблюдения права на свободу слова, соблюдения юридических обязанностей контролера по сбору персональных данных, а также ради «государственного интереса в области общественного здравоохранения» [2], в научных, исторических и архивных целях.

В российском законодательстве право на забвение не упоминается, но как право на исправление и удаление своих данных присутствует в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 10.3 обязывает оператора поисковой системы прекратить распространять недостоверную, неполную, неактуальную или же утратившую значение информацию, а также информацию, собранную незаконным путем.

Таким образом мы видим, что, с одной стороны, право на забвение уже заняло свое прочное место в законодательстве, а, с другой – оно сводится только к праву на удаление данных. При этом право на забвение может выступать комплексным инструментом защиты, выходящим за рамки простого удаления, и определяться «как право отдельных лиц лучше контролировать свои личные данные» [8. Р. 18].

II. Этические проблемы обработки персональных данных. Взаимодействие пользователей с платформами и сервисами в Интернете предполагает определенную схему и алгоритмизируется, что обусловлено необходимостью сбора данных, как предполагается, для более качественного взаимодействия с пользователем, анализа предпочтений и выявления тенденций. При этом сам процесс сбора, хранения, обработки и передачи данных регламентируется законодательно, а потому пользователю предлагается дать свое согласие на обработку персональных данных. Всегда есть отдельное условие, что согласие может быть отозвано в любой момент, с трудом реализуемое практически. Проиллюстрируем указанное положение дел с помощью мысленного эксперимента.

Представим себе такую ситуацию, что вас приглашают в гости на вечеринку. Вы заходите в дверь и попадаете внутрь квартиры, наполненной разными людьми. Вы с ними знакомитесь и весело проводите время, но вот пришла пора идти домой. Вы хотите выйти, а вам говорят, что выход через другую дверь. Вы направляетесь к двери, открываете ее, а за ней видите длинный лабиринт, по которому вы идете и не понимаете, как выбраться наружу. Или же за дверью вы видите болото, через которое вам придется пробраться, испачкавшись в тине, чтобы добраться до дома. Правильно ли поступил хозяин квартиры, устроив для вас такое испытание? Или же мы назовем его подлецом? Можем ли мы рассчитывать на такой же простой выход, как и на вход, когда нас завлекают куда-либо?

Эта ситуация аналогичная стандартной процедуре взаимодействия в Интернете:

1) пользователь дал свое согласие и пришел на вечеринку (дал согласие и подписал документы правил пользования сервисом/социальной сетью/приложением);

2) он знал изначально, что может уйти и его не будут держать (он прочел, что может отозвать согласие и как это сделать);

3) однако, ему ничего не сказали о том, насколько сложно будет найти выход (он столкнулся с непонятным и запутанным интерфейсом и дизайном, усложняющим поиск отзыва согласия, а также с бюрократическими препятствиями).

Возникает первый вопрос: правильно ли с точки зрения этики создавать дизайн сайта или приложения, затрудняющий человеку удаление собственных данных? Право на забвение может повлиять на развитие технологической отрасли в сторону создания более этичного и гуманного интерфейса сайтов и приложений, работающих с персональными данными. «Если дизайнеры не осознают существенного содержания создаваемых ими продуктов, их работа не принесет значимых результатов или даже может нанести вред в нашем сложном мире» [4. Р. 35]. Плохой дизайн становится не просто неудачным ходом конкретного предпринимателя, но приводит к негативным этическим и политическим последствиям для общества. Возможно, пришла пора расширить право на забвение в сторону регуляции принципов построения дизайна для платформ, собирающих персональные данные?

Другая проблема, заставляющая активистов говорить о праве на забвение, заключается в так называемых «сливах» или утечках информации. В последние несколько месяцев произошло несколько крупных утечек. В качестве примеров стоит вспомнить утечку из сервиса по доставке еды «Яндекс.Еда» [3] и медицинской лаборатории «Гемотеста» [1]. Появление в Интернете пользовательских данных из «Яндекс.Еды» привело к созданию карты, на которой отмечено конкретное местоположение с информацией о заказах, потраченных суммах, а также персональная информация пользователей (имена, места проживания, номера телефонов и т. д.). Компрометация приватной информации негативно воздействует как на последующее состояние пользователей (поскольку она может быть использована для мошенничества), так и предполагает сопутствующие репутационные риски, активизирующие алармистские настроения относительно невозможности обеспечения безопасного хранения данных. В случае утечки данных из «Гемотеста» обостряется еще один вопрос: медицинской информации.

Медицинская информация должна быть защищена особо, поскольку содержит в себе то, что может быть квалифицировано как врачебная тайна, а потому касающееся только врача и пациента. Утечка из «Гемотеста» представляет собой опасность не только персональными данными (как в случае «Яндекс. Еды»), но способно оказать большое влияние на дальнейшую жизнь человека в случае обнародования данных. Гипотетически, не только наличие заболеваний, которые возможно определить у конкретного человека, идентифицировав его с помощью утекших данных, способно негативно повлиять на существование человека (например, в случае таких стигматизирующих заболеваний, как ВИЧ-инфекция), но и сам факт обращения для проведения медицинского исследования отразится на жизни человека (например, при обследовании на венерические заболевания).

Две эти ситуации показывают, что на данный момент правовые нормы не могут обеспечить безопасность граждан и комфортную интернет-среду. Люди нуждаются в праве на забвение, чтобы вернуть власть над своей личной жизнью, своими персональными данными и своей идентичностью.

Причина, по которой возникает сама проблема утечек, состоит в проникновении технологий и алгоритмов в ткань человеческого существования. Как замечают М. Додж и Р. Китчин: «Всепроникающие вычислительные технологии нацелены на дополнение всех аспектов жизни и деятельности, стремясь повысить их ценность за счет добавления вычислительной мощности к повседневным объектам, делая их в определенной степени «умными», но в то же время обыденными и рутинными» [5. Р. 431]. Появление посредника, хранящего персональную информацию, приводит либо к появлению требований, предъявляемых к способам защиты данных. Одним из наиболее очевидных решений видится необходимость создания надежных механизмов защиты, но в условиях становящихся и изменяющихся технологий появление полностью надежной защиты невозможно. Поэтому другим требованием становится применение еще на уровне концептов и дизайна принципов, позволяющих пользователям, то есть тем, кто содержательно наполняет платформы, активно участвовать в судьбе тех данных, которые они передают. Речь идет о расширении информационной автономии, понимаемой как «способность делать выбор, принимать обоснованные решения; другими словами, сохранять контроль над определенными аспектами своей жизни» [7. Р. 86], которые касаются обработки и хранения информации и данных.

Другой возможный вариант решения данной проблемы – это расширение права на забвения на вопрос удаления всей информации пользователей по прошествии определенного времени в случае, если человек не пользуется сайтом. Технически это может быть выполнено в виде дополнительного согласия на удаление данных через определенный временной промежуток, которое пользователь подписывает вместе с согласием на обработку данных. Учитывая, что «увеличение количества данных, особенно в Интернете, повысила их экономическую ценность» [6. Р. 149], подобный подход даст гражданам больше контроля над ценными ресурсами, которые сейчас находятся во власти IT-корпораций.

Список литературы

1. «Гемотест» начал расследование об утечке данных 30 млн клиентов // РБК. URL: <https://www.rbc.ru/society/04/05/2022/6272665b9a794713ec6698dd> (дата обращения: 03.09.2022).
2. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27.04.2016 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС // Справочно-правовая система «Гарант». URL: <http://ivo.garant.ru/#%2Fdocument%2F71936226%2Fparagraph%2F379%3A0> (дата обращения: 12.09.2022).
3. Сервис «Яндекс.Еда» сообщил об утечке информации о клиентах // РБК. URL: https://www.rbc.ru/technology_and_media/01/03/2022/621e3b5e9a794716fef53d0 (дата обращения: 03.09.2022).
4. Buchanan R. Human Dignity and Human Rights: Thoughts on the Principles of Human-Centered Design // Design Issues. 2001. Vol. 17, № 3. Pp. 35–39.
5. Dodge M., Kitchin R. ‘Outlines of a World Coming into Existence’: Pervasive Computing and the Ethics of Forgetting // Environment and Planning B: Planning and Design. 2007. № 34(3). Pp. 431–445.
6. Mkadmi A. Archives in the Digital Age: Preservation and the Right, to be Forgotten. London, Hoboken: Wiley-ISTE, 2021.
7. Terwangne C. The Right, to be Forgotten and Informational Autonomy in the Digital Environment // The Ethics of Memory in a Digital Age. Palgrave Macmillan. 2014. Pp. 82–101.
8. Werro F. The Right, to Be Forgotten: The General Report – Congress of the International Society of Comparative Law, Fukuoka, July 2018 // The Right, to Be Forgotten: A Comparative Study of the Emergent Right’s Evolution and Application in Europe, the Americas, and Asia. Springer, 2020.

А. Фартушнова,
юрисконсульт ООО «Отель»

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ СРЕДЕ

Аннотация. В настоящее время в мире не предвидится какого-либо спада и тем более остановки в технологическом развитии и совершенствовании вычислительных систем, в развитии технических средств связи, цифровой среды. Темпы развития информационно-технологических средств на сегодняшний день в Российской Федерации существенно превышают скорость совершенствования и адаптации соответствующей нормативно-правовой базы. Большая часть существующих нормативно-правовых актов направлена на правила поведения в цифровой среде. Однако, по большому счету, отсутствуют развитая культура цифрового общения и взаимодействия и практика применения действующих норм права. Среди действующих нормативных правовых актов не слишком много норм, существенно регулирующих ответственность за на-

рушение информационной безопасности граждан, общества и государства. Актуален и вопрос кодификации уже существующих нормативно-правовых актов.

Ключевые слова: информация, информационная безопасность, гражданин, общество, государство, право, цифровая среда, защита

LEGAL REGULATION INFORMATION SECURITY IN THE DIGITAL ENVIRONMENT

Abstract. At present, the world does not expect any recession and, moreover, a stop in technological development and improvement of computing systems, in the development of technical means of communication, the digital environment. The pace of development of information technology tools today in the Russian Federation significantly exceeds the rate of improvement and adaptation of the relevant regulatory framework. Most of the existing regulations are aimed at the rules of conduct in the digital environment, in particular. However, by and large, there is no such thing as just a culture of digital communication and interaction, as well as the practice of applying the existing rules of law. Among the current regulatory legal acts there are not too many norms that significantly regulate the responsibility for violating the information security of citizens, society and the state. The issue of codification of already existing legal acts is also relevant.

Keywords: Information, Information Security, Citizen, Society, State, Law, Digital Environment, Protection

Введение. Понятие «информационная безопасность» давно «шагнуло вперед». С началом активного развития информационных технологий и возможностью выхода практически каждого жителя планеты Земля из любой ее точки в глобальную сеть «Интернет» информационная безопасность перестала быть локальной – ограниченной исключительно определенной территорией и выходящей за пределы такой территории только с одновременным передвижением владельца той или иной информации.

Сейчас любая информация, попавшая в Интернет, мгновенно «расходится» по ряду лиц – от ограниченного числа лиц до неограниченного ничем круга таковых.

Уже при первом выходе в сеть «Интернет» и соответствующей аутентификации каждый пользователь априори приобретает свое так называемое «цифровое я». Помимо части этого «цифрового я» пользователя, формируемой волей самого пользователя (будь то добровольная выкладка собственных фотографий, размещение видеозображений, отправка аудио-сообщений, просто какой-либо, в том числе частного характера, информации и пр.), «цифровое я» каждого человека постоянно наполняется попутно собираемой и постоянно обрабатываемой информацией (сведениями об интересах, увлечениях, потребностях, покупках, приоритетах, местах обучений, связях с другими лицами и пр.), где куки-файлы, к примеру, являются самими «безобидными». Сторонними лицами может дополнительно осуществляться и целенаправленный сбор информации о человеке – как санкционированный, так и не отвечающий требованиям действующего законодательства. Во всех случаях чем больше «цифровое я» пользователя наполняется

информацией, тем фундаментальной формируется его «второе я» в цифровой среде, что влечет за собой и скрытую опасность – гражданин в условиях все большей и повсеместной цифровизации рискует утратить свои человеческие права, а его «цифровое я» становится вектором существования гражданина, при воздействии на который с должной легкостью становится возможным управлять повседневной жизнью человека.

Основная часть. Защита информации – одна из задач государства. Обеспечение информационной безопасности граждан, общества в целом – должно всегда оставаться в приоритете всех стран.

Последние годы было принято считать, что Соединенные Штаты Америки, как «локомотив» в сфере мирового развития информационных технологий, по умолчанию имеют и наиболее прогрессивные правовые решения и практику применения норм права в области информационной безопасности в цифровой среде. Однако миру известны не единичные случаи, когда именно в инициативах США блокировались страницы в социальных сетях высокопоставленных лиц США, а судебная система создавала прецедент, в рамках которого публичной личности не удавалось защитить своих прав против созданных на нее (такую личность) с использованием нейросетей дипфейков.

Информация представляет из себя некие сведения. Обеспечение безопасности тех или иных сведений, логично, должно быть направлено на их сохранность, прежде всего, в частности, на защиту от несанкционированного распространения и передачи. Но также не менее важно обеспечивать и защиту и от самой информации. До специальной военной операции в Донецкой и Луганской народных республиках, начатой Российской Федерацией 24 февраля 2022 г., устойчивым было мнение, что защищать от деструктивной информации необходимо детей. Однако начало специальной военной операции ярко показало, что в защите от информации в любом государстве и обществе нуждаются не только дети, но и взрослые граждане. С развитием информационных технологий и совершенствованием цифровой среды, можно смело утверждать, что информация в любой момент времени становится оружием массового поражения, средством криминального и даже террористического воздействия.

Принимая во внимание тот факт, что в условиях глобализации информационные технологии беспрепятственно развивались без обязанности быть привязанными к тому или иному государству территориально, это естественным образом влекло за собой и все риски нарушения информационных внутригосударственных инфраструктур даже без физического территориального вмешательства.

Известно, что все большое начинается с малого. Прежде всего, когда в обществе информационные технологии развиваются семимильными шагами, цифровизация охватывает все области жизни, включая социальные сферы, военные и т. д., отсутствие в том же обществе «цифровой культуры» не способствует укреплению и информационной безопасности. Мало кто из граждан той или иной страны придает должное значение тому, что и на каких условиях он размещает своими силами в сети «Интернет» – на любом ресурсе, не принадлежащем пользователю.

Все больше в России говорят о том, чтобы вводить в практику цифровые паспорта. Однако каким образом с правовой точки зрения уже сегодня можно обеспечить тотальную безопасность таким паспортам, не совсем понятно.

Так, например, дактилоскопия признает, что редко, но отпечатки на подушечках пальцев у разных людей совпадают. Уникальной считается сетчатка глаза. Учеными было выяснено, что вероятность второго совпадения при аутентификации по сетчатке глаза не превышает одного процента.

Если предположить, что для обеспечения наибольшей защиты каждого гражданина Российской Федерации в цифровом профиле паспорта гражданина аутентификация будет возможна по сетчатке глаза, то непонятым становится, каким образом «вернуть», изъять по всему миру все высокого качества цифровые изображения гражданина из обработки (хранения, использования и пр.). По фотографии хорошего качества технически (без подогрева до температуры тела человека) возможно произвести и подлог. Возможность же предусмотреть температуру тела одновременно при аутентификации влечет за собой сложности для владельца паспорта в условиях холода либо лихорадки и т. д. Круг замыкается. Плюс к этому, к примеру в некоторых крупных городах Российской Федерации на парадных многоквартирных домов установлены домофоны с возможностью любому жителю той или иной парадной сохранять видеофрагменты с камер домофона и далее их передавать. А в ряде мест временного проживания вход на территорию отелей осуществляется по отпечаткам пальцев. При этом обработкой отпечатков и прочих персональных данных сотрудников таких отелей занимается работодатель в лице как минимум руководителей штатных структур, системных администраторов и пр.

Помимо отсутствия «цифровой культуры» пользователей в обычной жизни, такое явление повсеместно распространено и в профессиональной среде: часто можно наблюдать в поликлинике картину, когда медицинский работник, например, ошибочно либо неровно распечатывает персональные данные пациента и ненужный лист с такими данными просто выбрасывает в урну, даже, элементарно, не удосуживаясь лист с чужими данными хотя бы разорвать; похожие ситуации часто происходят и в других органах публичной власти.

Большие данные результатов цифрового профилирования людей в руках злоумышленников становятся инструментом давления на общество и власть. Они способны влиять на массовое сознание людей, на образ их жизни и, как следствие, способны приводить к дестабилизации даже внешне стабильного общества, вплоть до инициирования вооруженных столкновений, приводить к ослаблению суверенитета целых государств.

В виду того, что интернет-среда в современном обществе не может тотально подавляться, в чем нет и никакой объективной необходимости, цифровая среда в сети «Интернет» может представлять из себя «надгосударственную» организованную структуру, прежде всего, в той стране, где «цифровая культура» либо полностью отсутствует, либо слабо развита.

Простой пример, когда в 2022 г. в некоторых органах публичной власти Российской Федерации, в частности, как видно из открытых источников при соответствующем запросе в поисковой цифровой среде, действующим правительством Санкт-Петербурга было запрещено своим подчиненным пользоваться таким мессенджером, как WhatsApp, но одновременно было рекомендовано пользоваться Telegram. При этом тот факт, что братья – владельцы Telegram лишь по факту рождения имеют отношение к Российской Федерации, а штаб-квартира Telegram распо-

лагается в Англии, операционный центр – в ОАЭ, часть серверов – на территории США, действующими властями Санкт-Петербурга был полностью проигнорирован, в лучшем случае по незнанию.

Впервые в Российской Федерации в действие за неправомерное воздействие на критическую информационную инфраструктуру России была введена ответственность ст. 274.1 Уголовного кодекса Российской Федерации [1].

Об отставании права от развития цифровых технологий тоже ярко свидетельствуют, например, факт принятия Президентом Российской Федерации Указа № 490 «О развитии искусственного интеллекта в Российской Федерации», изданного лишь 10 октября 2019 г., или Федеральный закон Российской Федерации № 123-ФЗ «О проведении эксперимента ... для разработки и внедрения технологий искусственного интеллекта в ... городе Москве...» от 24 апреля 2020 г. [2, 3]. Только с этих годов в Российской Федерации впервые регламентируется понятие «искусственного интеллекта», в то время как уровень развития и «обучения» искусственного интеллекта технологически уже достиг больших результатов, в том числе в медицине, в военном обеспечении и т. д.

Заключение. Безусловно, одной из обязанностей каждого государства является обязанность по обеспечению безопасности граждан в стране, включая информационную безопасность. Тем более важно одновременное развитие информационных технологий, своевременное совершенствование нормативно-правовой базы и практики применения последней и обеспечение органами публичной власти обучения «цифровой культуре» граждан, начиная с детского возраста и «с самих себя».

В условиях многополярного мира также важно выработать общие четкие соответствующие международные нормы права, направленные на взаимоотношения граждан разных стран и взаимоотношения государств между собой в условиях глобальной цифровой среды, безукоснительное выполнение которых будет способствовать, прежде всего, информационной безопасности как отдельно взятого индивидуума, так и мира в целом.

Список литературы

1. Уголовный кодекс Российской Федерации: текст с изменениями и дополнениями на 25 июля 2022 г.: [принят Государственной Думой 24 мая 1996 г.: Одобрен Советом Федерации 05 июня 1996 г.]. Москва. URL: <https://online.consultant.ru/riv/cgi/online.cgi?req=doc&ts=XEFmDETKx4yo0eCG1&cacheid=7F89DE13DC55587E506A7D69FFDCEE9B&mode=splus&rnd=E9ljA&base=LAW&n=422137&dst=101786#xmXREETmW6rH2Kn52>: Режим доступа: Правовая электронная база «КонсультантПлюс» с доступом по онлайн-паролю: дистрибьютор ООО «Ваше Право».

2. 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»: Федеральный закон № 123-ФЗ: [принят Государственной Думой 14 апреля 2020 г.: одобрен Советом Федерации 17 апреля 2020 г.]. Москва, Кремль. URL: <https://online.consultant.ru/riv/cgi/online.cgi?req=doc&ts=nbRnmBTeCnM5pSUL1&cacheid=DF9F69020F63DEF647E13159A898C>

BF6&mode=splus&rnd=KKkZGw&base=LAW&n=351127#5rWnmBT2zGYpcQaH1:
Режим доступа: Правовая электронная база «КонсультантПлюс» с доступом по онлайн-паролю: дистрибьютор ООО «Ваше Право».

3. Указ Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» № 490: утв. Президентом Российской Федерации 10 октября 2019 г. URL: <https://online.consultant.ru/riv/cgi/online.cgi?req=doc&ts=XEFmDETKx4yo0eCG1&cacheid=C7768633A8250F9B30C884C22F1DE63C&mode=splus&rnd=E9ljA&base=LAW&n=335184#DCxEETo9kBD3kKC2>:
Режим доступа: Правовая электронная база «КонсультантПлюс» с доступом по онлайн-паролю: дистрибьютор ООО «Ваше Право».

Р. В. Федоров,

кандидат юридических наук, доцент,
Российский технологический университет

ТЕОРЕТИКО-ПРАВОВЫЕ АСПЕКТЫ МЕТОДА ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ТЕКСТА И ДАННЫХ

Аннотация. Статья посвящена исследованию феномена майнинга данных (text & data mining). Определяются возможные направления юридических научных исследований этого явления. В результате проделанной работы делается вывод, что проблема правового регулирования майнинга данных является весьма актуальной в мире, а значит и в его неотъемлемой части – России и требует детальной научной разработки в целях повышения конкурентоспособности нашей страны.

Ключевые слова: майнинг данных, TDM, информационное право, искусственный интеллект, машинное обучение, невыразительные данные, авторские права

THEORETICAL AND LEGAL ASPECTS OF THE TEXT AND DATA MINING

Abstract. The article is devoted to the study of the phenomenon of data mining (text & data mining). The author defines possible directions of legal scientific research of this phenomenon. As a result of the work done, the author concludes that the problem of legal regulation of data mining is very relevant in the world, and therefore in its integral part – Russia and requires detailed scientific development in order to increase the competitiveness of our country.

Keywords: Data mining, TDM, Information law, Artificial intelligence, Machine learning, Featureless data, Copyright

В XXI в. значение информации подобно значению нефти в XVIII в.: она является чрезвычайно ценным и малоиспользуемым активом. Как и в случае с нефтью, тех, кто видит фундаментальную ценность данных и учится извлекать и использовать их, ждет огромная награда [1].

Вот уже несколько лет мы слышим, что «данные – это новая нефть». На самом деле, это утверждение, каким бы гиперболическим оно ни звучало, является

редукционным. Нефть – это родовая потребляемая вещь, ограниченный ресурс, и в настоящее время единодушно признается настоятельная необходимость как можно быстрее заменить ее в качестве источника энергии. Данные, с другой стороны, не являются взаимозаменяемыми, учитывая, что фрагменты данных отличаются друг от друга, они никогда не иссякнут и, наоборот, будут увеличиваться экспоненциально с течением времени, тем самым возрастая в цене. Более того, для промышленности, ученых и даже для целых стран данные становятся все более необходимыми.

Таким образом развитие частных компаний и государств в целом вскоре будет сильно зависеть от умения использовать и обрабатывать данные с целью получения выгод и преимуществ.

Поскольку анализ данных (в том числе и текстов) включает в себя различные правовые аспекты, такие как защита интеллектуальной собственности и персональных данных, то результат такого анализа будет в значительной степени зависеть от создания качественной правовой базы, обеспечивающей надлежащий баланс интересов в данной сфере деятельности, способной защитить интересы правообладателей и, в то же время, обеспечить возможность свободного использования преимуществ этих новых технологий, не создавая ненужных препятствий для этого.

Указанные вопросы требуют правового исследования. Прежде всего следует сосредоточить внимание на общественных отношениях по поводу интеллектуальной собственности, на феномене интеллектуального анализа текста и данных (майнинг данных, англ.: text & data mining, далее по тексту – TDM). Этот термин (TDM) используется для описания «любого автоматизированного аналитического метода, направленного на анализ текста и данных в цифровой форме с целью получения информации о закономерностях, тенденциях и корреляциях» [2].

Правовое регулирование майнинга данных является достаточно сложным вопросом. Это все еще относительно неисследованная область знаний о которой мало что написано, но которая охватывает сразу несколько правовых областей таких как: авторское право, информационное право, договорное право, международное право, конкурентное право. Кроме того, тема касается и этических вопросов, таких как защита персональных данных.

Исследование вопросов правового регулирования майнинга данных следует начинать с описания феномена интеллектуального анализа текста и данных в его «технических» аспектах. Далее, после обзора истории рассматриваемого вопроса от самых отдаленных времен и до рождения Интернета и появления категории «больших данных», учитывая рост интереса к искусственному интеллекту (ИИ) во всем мире за последние 30 лет, будет нелишним попытаться оценить стоимость отрасли как в микро-, так и в макроэкономическом плане. Большой объем исследования должно занять техническое объяснение типа данных, которые могут быть использованы в процессе TDM. Безусловно глубокого анализа требуют юридические вопросы, которые могут возникнуть в связи с применением таких методов, особенно в рамках законодательства об интеллектуальной собственности (авторского права и защиты баз данных) и в области защиты персональных данных.

Вероятно, авторское право станет основным правовым барьером, который будет существенно препятствовать деятельности по интеллектуальному анализу текстов и данных, эту проблему необходимо подробно исследовать, принимая

во внимание историю постоянного противоборства в течение последних 300 лет между идеями о необходимости защиты авторских прав и потребностями в научных инновациях. Очевидно, что эти непростые отношения (также известные как «войны за авторское право») всегда характеризовались сближением большого разнообразия интересов, стоящих на кону, и явно циклическим характером. При этом важность и вес авторского права в современном обществе увеличивается.

Интерес представляет исследование зарубежных теорий защиты авторских прав, в том числе в рамках правовых традиций гражданского права и англо-саксонского общего права, широко известных в международном сообществе и обобщенных как «естественное право» и «утилитаристская теория». Здесь мы обнаруживаем основополагающее различие в подходе, которое имеет большое значение для построения системы авторского права. Речь идет об особенностях формирования самих прав и особенно исключений из них – открытых исключений и конкретных (прямых) исключений. Эти аспекты особенно важны, так как они помогут лучше понять различия в механизмах правового регулирования технологий интеллектуального анализа текста и данных.

Сосредоточившись на истории авторского права с самого его зарождения и до наших дней, следует попытаться выявить причины и определить основные события, которые привели к сегодняшнему результату, когда такая деятельность, как интеллектуальный анализ текста и данных, которые можно охарактеризовать как «невыразительные» или «непотребляемые», в конечном итоге создает результат, подлежащий включению в сферу регулирования авторских прав.

Отдельного внимания следует уделить анализу структуры авторских прав и исключений из них, а также директиве о базах данных, действующую в Европейском союзе. Это позволит лучше понять, почему авторские права следует считать потенциальным препятствием для работы с текстом и интеллектуального анализа данных. За последнее десятилетие некоторые европейские страны ввели отдельные исключения, посвященные деятельности по интеллектуальному анализу текста и данных. Исследование этих законодательных инициатив также может быть полезным.

Следует отметить, что для регулирования процесса интеллектуального анализа текста и данных Европейский союз решил предпринять два различных подхода: первый – подход к лицензированию, который оказался неудачным; второй – подход, основанный на исключениях.

Анализа требует и законодательный процесс, который привел к принятию Директивы о едином цифровом рынке и, благодаря ей, к окончательному введению двух конкретных исключений для деятельности TDM в европейской системе авторского права: ст. 3, адресованная субъектам, участвующим в научных исследованиях, и ст. 4, которая приносит пользу более широкому кругу пользователей. Внимания заслуживает реакция и критика, высказанная в отношении этих двух исключений, возникшая после их внедрения в государствах-членах ЕС, а также альтернативные решения для реформирования европейского авторского права, за которые выступают некоторые ученые.

Наконец, TDM следует рассмотреть с точки зрения сравнения различных подходов, которых придерживаются страны за пределами Европы, в первую оче-

редь – в Соединенных Штатах Америки. Особое внимания заслуживают также Япония, Тайвань, Южная Корея, Израиль, Австралия и Канада, а также Китай.

Таким образом, проблема правового регулирования майнинга данных является весьма актуальной в мире, а значит, и в его неотъемлемой части – России и требует детальной научной разработки в целях повышения конкурентоспособности нашей страны.

Список литературы

1. Директива об авторском праве на Едином цифровом рынке Европейского Союза. URL: <https://eur-lex.europa.eu/eli/dir/2019/790/oj> (дата обращения: 14.09.2022).

2. Toonders J. Data Is the New Oil of the Digital Economy, Wired. URL: <https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/> (дата обращения: 14.09.2022).

О. А. Харина,

кандидат политических наук, научный сотрудник,
доцент департамента зарубежного регионоведения
факультета мировой экономики и мировой политики,
Национальный исследовательский университет
«Высшая школа экономики»

ЦИФРОВИЗАЦИЯ ПОЛИТИКИ В ИНДИИ: ОПЫТ ДЛЯ РОССИИ

Аннотация. В условиях трансформации представляется крайне важным изучение опыта цифровизации азиатских гигантов, которые являются одними из основных поставщиков высокотехнологичных продуктов, их практическое применение влияет на характер и будущее промышленной революции в различных государствах. Рассматриваемый в работе опыт Индии показывает, что она достигла успешного перехода к цифровой составляющей в различных сферах жизни. В настоящее время Индия стала второй по скорости внедрения цифровых продуктов и одной из крупнейших цифровых экономик мира. С момента внедрения программы «Цифровая Индия» в 2015 г. до сегодняшних дней произошло много существенных улучшений в цифровой инфраструктуре. Целью работы является анализ государственных и банковских услуг, а также повышения информационной грамотности населения Индии. Научная новизна работы состоит в возможной адаптации успешного опыта Индии для Российской Федерации с целью повышения эффективности ее политики.

Ключевые слова: Индия, Россия, сотрудничество, цифровизация, информационное общество, цифровая экономика, цифровизация политики

DIGITALIZATION OF POLITICS IN INDIA: EXPERIENCE FOR RUSSIA

Abstract. In the context of transformation, it seems extremely important to study the experience of digitalization of Asian giants, which are among the main suppliers of high-tech products, their practical application affects the nature and future of the industrial

revolution in various states. The experience of India considered in this paper shows that it has achieved a successful transition to the digital component in various spheres of life. Currently, India has become the second fastest digital product adoption and one of the largest digital economies in the world. Since the introduction of the Digital India program in 2015 to the present day, there have been many significant improvements in the digital infrastructure, the purpose of the work is to analyze government and banking services, as well as to increase information literacy of the Indian population. The scientific novelty of the work consists in the possible adaptation of the successful experience of India for the Russian Federation in order to increase the effectiveness of its policy.

Keywords: India, Russia, Cooperation, Digitalization, Information society, Digital economy, Digitalization of politics

Пандемия коронавируса продемонстрировала особенную важность цифровой инфраструктуры, которая указала на необходимость развития IT-технологий. Мир стал зависимым от непрерывной работы гаджетов и высокотехнологичных устройств, особенно от ПК, поскольку обучение и работа перешли в онлайн-плоскость, а «облачная» инфраструктура стала основным местом для хранения и обеспечения доступа к файлам и документам. Всемирная сеть Интернет предоставляет все больше необходимых для повседневной жизни предложений гражданам, крупным и мелким предприятиям, а также государственным структурам.

Республика Индия перешла к цифровой трансформации в 2015 г., когда премьер-министр Нарендра Моди запустил программу «Цифровая Индия» [12], и к 2022 г. она уже дала результаты, связанные с внедрением цифровых технологий в разных сферах жизни населения. Общее число пользователей сети Интернет в Индии в 2020 г. превышало количество аналогичных пользователей в некоторых развитых странах [10]. Успех Индии на данном направлении и возможность заимствования Россией ее опыта обуславливают актуальность исследования.

Целью данной работы является анализ государственных и банковских услуг, а также повышение информационной грамотности населения Индии.

Тема исследования разрабатывалась различными учеными, однако не в полной мере. Они рассматривали влияние цифровизации на отдельные сферы экономики и на бизнес-среду. Среди российских авторов особенно выделяются работы Н. А. Мартыновой [4], А. А. Гуцалова [2], а также Л. В. Кулик [3]. Зарубежные авторы анализируют промежуточные результаты программы цифровизации в Индии, однако фундаментальные работы, нацеленные на оценку возможного сотрудничества России и Индии в области цифровых технологий, отсутствуют.

Теоретическую базу исследования можно разделить на три основные части: статистические источники (данные официального сайта программы «Цифровая Индия», Министерства науки и технологий Индии, заключения комиссий, нормативно-правовые акты в области цифровизации), работы исследователей, таких как И. Андропова [1], В. А. Перминов [7], В. В. Смирнов [8], направленные на изучение этапов цифровой трансформации в Индии, а также труды авторов, которые занимаются исследованием российско-индийских отношений в сфере инвестиций и экономики, например Е. В. Чудинова [9].

В исследовании используется комбинация различных методов, среди которых метод анализа (выделение особенностей процессов цифровизации и их изучение), системный подход (рассмотрение программ как части общей политики Индии) и метод сравнения (сопоставление двух моделей государств и выделение возможностей для кооперации).

Гипотеза в работе сформулирована следующим образом: программа «Цифровая Индия» является успешным проектом, образец которого может быть использован другими государствами для осуществления подобной практики, в частности, Россией.

E-Participation в Индии. Digital India (перевод с английского: «Цифровая Индия») представляет собой крупный государственный проект, объединяющий различные усилия в области подключения населения к сети Интернет, повышения информационной культуры и перевод на более высокий уровень цифрового управления [10].

На сегодняшний день в Индии реализуются семь программ в рамках проекта «Цифровая Индия», которые направлены на упрощение доступа граждан к сервисам и услугам ведомств, а также учитывают все современные достижения науки и технологий.

С 2000-х гг. Правительство Индии стремится быть более доступным для своих граждан с помощью различных общественных инструментов, таких как социальные сети, портал открытого управления. Расширяется практика использования сайтов и приложений, посвященных вопросам управления (коррупция, насилие в отношении женщин и т. д.).

В 2006 г. Правительством Индии был принят Национальный план электронного управления (National e-Governance Plan). Он включает в себя развитие инфраструктуры предоставления сервисов электронного правительства (National State Service Delivery Gateway), инфраструктуры доступа в Интернет (State Wide Area Networks), государственных дата-центров (State Data Centres), а также центров обслуживания населения (Common Services Centers) и специальных электронных форм доставки услуг (e-Forms).

Динамика E-Participation в Индии показывает, что в государстве на высоком уровне развиты:

1. Доступ граждан к публичной информации, к информации по запросу.
2. Привлечение граждан к участию и обсуждению государственной политики и услуг.
3. Возможность населения участвовать в совместной разработке вариантов государственной политики, в оказании услуг и способов их предоставления [5. С. 131].

Рост цифровых и высоких технологий стимулировал развитие системы электронного управления в системе государственного управления в Индии.

Запущенные ранее инициативы, такие как Национальный план электронного управления (2006 г.), Национальная оптоволоконная сеть (2011 г.) и Агентство Индии по уникальной идентификации (2009 г.), были изменены, а «Цифровая Индия» стала брендом и национальной идеей. Премьер-министр Индии Н. Модди, говоря о данном проекте сказал: «Наша мечта – это “Цифровая Индия” для бедных, а не только для элиты. Мы стремимся дать каждому ребенку, даже в самых отдаленных деревнях страны, полноценное образование. Мы стремимся к тому, чтобы каждый

гражданин имел возможность использовать свои телефоны для ведения банковского счета, взаимодействия с правительством, удовлетворения своих повседневных потребностей и ведения бизнеса на ходу. А для этого мы должны отправиться в цифровую Индию» [10].

Усилия Правительства Индии по активизации национальной программы биометрической цифровой идентификации «Опора» (Aadhaar) привели к позитивным результатам внедрения. С момента появления в «Опора» приняли участие 1,2 млрд человек, что сделало ее самой крупной программой цифрового удостоверения личности в мире и ускорило распространение других цифровых услуг [12]. По числу цифровых потребителей Индия является одной из крупнейших и наиболее быстрорастущих в мире стран, а также осуществляет цифровизацию быстрее, чем многие страны с развитой экономикой.

Согласно анализу компании Мак-Кинзи, в основе которого были данные технологического роста государств по 30 параметрам внедрения цифровых технологий с 2014 по 2018 г., Индия осуществляет цифровизацию быстрее, чем все страны, участвующие в исследовании, кроме одной – Индонезии. Показатель Индии с 2014 по 2018 г. вырос на 90 % [14].

Изменения, вызванные внедрением цифровых технологий, модифицируют рынок труда. Новые рабочие места создаются в результате прямого и косвенного воздействия цифровых приложений, повышающих производительность и качество предоставляемых услуг. Рабочие места могут быть открыты в таких отраслях, как строительство и производство, сельское хозяйство, торговля и гостиничный бизнес, финансы, СМИ и телекоммуникации, а также транспорт и логистика.

Несмотря на все преимущества и успехи внедрения цифровых технологий, с 2015 по 2022 г. в программе по цифровизации в Индии было немало сбоев, начиная с многочисленных петиций, ставящих под сомнение конституционность «Опоры», которая имеет доступ к персональным данным граждан.

Особенности E-participation в России. Цифровизация является одним из главных приоритетов развития для России. Во время выступления в Госдуме в 2020 г. премьер-министр РФ М. Мишустин заявил: «Цифровые технологии – это нефть, золото и платина XXI в. Если мы не перейдем к цифровым технологиям, они нас достанут» [6].

В России значительные усилия по цифровизации российской экономики стали предприниматься Правительством начиная с 2008 г. Именно в данный период в стране стали осуществлять значимые шаги по внедрению широкополосного Интернета в различных регионах страны. В 2010 г. в России отсутствовал законодательно утвержденный перечень государственных и муниципальных услуг, оказываемых в электронном виде, не был решен вопрос о признании на законодательном уровне электронного документа эквивалентом бумажного документа, существовала разрозненность государственных информационных ресурсов.

Система «Открытое правительство» получила свое начало в 2012 г. Основными значимыми достижениями этого проекта к 2017 г. стали:

Базовые основы новой информационной культуры взаимоотношений власти и граждан.

Развивающиеся технологии взаимодействия граждан и субъектов хозяйственной деятельности с государством.

Высокое качество и оперативность осуществления государственных функций и предоставления услуг.

Внедрение цифровых технологий в России не только открывает возможности, но создает риски в области защиты персональных данных, кибербезопасности и защиты информации. Среди перспективных направлений в Российской Федерации видится развитие центра передового опыта, который может заниматься инкубацией местных инноваций, упрощением технологических тенденций и продвижением технологического развития в области управления путем объединения дополнительных информационных ресурсов.

Опыт для России. В РФ разработана Национальная технологическая инициатива (НТИ) – долгосрочная программа, направленная на обеспечение лидерства российских компаний на новых высокотехнологичных рынках, которые появятся в мировой экономике в течение следующих 15–20 лет.

Как и в Индии, в России готовятся к тестированию и развертыванию сетей 5G. В настоящее время запущена национальная программа «Цифровая экономика» (до 2030 г.). НТИ и другие усилия России в технологической сфере и по обеспечению цифровизации могут быть согласованы со стратегическими планами Индии в аналогичных областях.

Опыт Индии в области цифровизации мало изучен в России. Важно отметить и то, что российские и индийские IT-технологии развиваются в разных темпах. При этом открываются новые элементы взаимодополняемости и перспективы сотрудничества между государствами. Так, успешный опыт Индии был применен в создании аналогичной структуры в РФ. Например, Российская ассоциация компаний – разработчиков программного обеспечения была создана по примеру Индийской национальной ассоциации компаний – разработчиков программного обеспечения и сервисных компаний.

Несколько инвестиционных фондов российского происхождения работают с Индией, стремясь объединить российский, индийский и международный опыт. К ним относятся Sistema Asia Capital, RTP Global, DST Global.

У двух государств есть потенциал для сотрудничества в области искусственного интеллекта, аналитики, интеллектуальной энергетической инфраструктуры, интеллектуальной логистики, фотоники, микроэлектроники и финансовых технологий.

Индия имеет уникальный опыт масштабирования низкомаржинальных продуктов и услуг. Сегодня индийские компании очень активно выходят на мировой рынок и могут служить трамплином для выхода российских решений на международные рынки.

Несмотря на достижения в цифровизации, Индия нуждается в дополнительных мерах и поддержке со стороны Правительства. На сегодняшний день только около 40 % населения имеют интернет-подписку. Около 90 % всех розничных транзакций в Индии по-прежнему совершаются наличными. Доходы от электронной коммерции растут более чем на 25–30 % в год, но при этом только 5 % торговли в Индии осуществляется через Интернет [7. С. 122].

Цифровая экономика Индии оценивается в сумму 200 млрд долл. США и является важной частью ее взаимодействия с миром, также она связана с перестановками и комбинациями в новых региональных и международных альянсах. Трудности «Цифровой Индии» заключаются в том, что программа и ее инициативы недостаточно совершенны и проработаны. Однако сам бренд остается привлекательным, поскольку он связан как с населением страны, так и с предпринимателями, которые пользуются преимуществами цифровизации.

Основные выводы. Программа внедрения современных технологий в Индии имеет ряд преимуществ, однако не может всецело считаться идеальной для применения. Но указанные выше проблемы и недостатки могут учитываться другими государствами, и она сможет применяться в модифицированном виде.

В контексте быстрого развития технологий и снижения стоимости передачи данных технологии, направленные на поддержку бизнеса, могут стать повсеместными в течение следующего десятилетия.

Опыт Индии имеет большую практическую значимость для России, поскольку обе страны разделяют тесное политическое партнерство и переживают аналогичную и довольно взаимодополняющую перестройку технологического сектора. Приверженность российского руководства цифровой трансформации как национальному приоритету, подкрепляющаяся модернизацией в ключевых секторах экономики, ориентированных на достижение конкретных результатов, позволит государству в будущем войти в группу лидеров цифровой трансформации, начать технологический прорыв и получить соответствующие преимущества в бизнесе и социальной среде.

Существующие цифровые инициативы в управлении государством и реализации государственных программ в Индии и России достигли успехов в предоставлении государственных услуг, региональном управлении, образовании, здравоохранении и других сферах. При этом важно отметить, что данные цифровые инициативы не должны ограничиваться исключительно ведомственными интересами. Сохранение граждан государства в качестве ядра и базы системы электронного управления способствовало бы достижению еще более устойчивых показателей экономики, где цифровые технологии выступают в качестве целесообразного средства, а не цели. Россия и Индия в данном контексте являются взаимодополняющими партнерами в формировании нового цифрового мира, и, если их усилия будут объединены, это принесет пользу развитию не только отдельных сфер жизни, но и двухсторонним отношениям в целом.

Список литературы

1. Андропова И. Государственная поддержка науки, технологий и инноваций в Индии // Мировая экономика и мировые отношения. 2019. № 11. С. 38–45. URL: <https://dlib.eastview.com/browse/doc/55985754> (дата обращения: 18.08.2022).
2. Гуцалов А. А. Опыт Индии в области цифровизации культуры: препринт Южного филиала Института наследия. Сер.: Теория и история культуры. Краснодар: Южный филиал Института наследия, 2020. 23 с.
3. Кулик Л. В. Инновации по-индийски // Российский совет по международным делам. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/innovatsii-po-indiyski/> (дата обращения: 10.05.2022).

4. Мартынова Н. А. Цифровые технологии в государственном управлении: опыт России и Республики Индия // Среднерусский вестник общественных наук. 2019. № 1. С. 127–143. URL: <https://cyberleninka.ru/article/n/tsifrovye-tehnologii-v-gosudarstvennom-upravlenii-opyt-rossii-i-respubliki-indiya> (дата обращения: 18.08.2022).

5. Мартынова Н. А., Хмельков, А. Б. Цифровые технологии в государственном управлении: опыт России и Республики Индия // Среднерусский вестник общественных наук. 2019. Т. 14, № 1. С. 127–144.

6. Мишустин назвал цифровые данные «нефтью, золотом и платиной» XXI века. URL: <https://iz.ru/986140/2020-03-12/mishustin-nazval-tcifrovye-dannye-neftiu-zolotom-i-platinoi-21-veka> (дата обращения: 21.08.2022).

7. Перминов В. А. Развитие умных городов в Индии // Российский внешнеэкономический вестник. 2020. № 8. С. 120–125. URL: <https://elibrary.ru/item.asp?id=43992121> (дата обращения: 18.07.2021).

8. Смирнов В. В., Мулендеева А. В. Использование информационных и коммуникационных технологий: Россия в сравнении с Индией, Китаем и США // Экономический анализ: теория и практика. 2019. № 2. С. 308–326. URL: <https://cyberleninka.ru/article/n/ispolzovanie-informatsionnyh-i-kommunikatsionnyh-tehnologiy-rossiya-v-sravnenii-s-indiey-kitaem-i-ssha> (дата обращения: 18.07.2022).

9. Чудинова Е. В. Государственное регулирование информационных технологий: Индия и Россия // Международный журнал гражданского и торгового права. 2019. № 1. С. 48–53. URL: <https://elibrary.ru/item.asp?id=37627449> (дата обращения: 18.07.2021).

10. 6 Years of Digital India: How successful has PM Modi's plan been? URL: <https://www.orfonline.org/research/6-years-of-digital-india-how-successful-has-pm-modis-plan-been/> (дата обращения: 10.05.2022).

11. Country Comparison. Internet users. TOP 100 (2020) // Index Mundi. URL: <https://www.indexmundi.com/g/r.aspx?t=100&v=118> (дата обращения: 24.08.2022).

12. Digital India // The Government of India. New Delhi. URL: <https://www.digitalindia.gov.in> (дата обращения: 24.08.2022).

13. Digital India: Technology to transform a connected nation. URL: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation> (дата обращения: 22.04.2022).

14. Global digital report 2018. URL: <https://wearesocial.com/blog/2018/01/global-digital-report-2018/> (дата обращения: 10.08.2022).

А. Д. Цветкова,

студент,

Уральский государственный юридический
университет имени В. Ф. Яковлева

СФЕРЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ КЕЙЛОГЕРОВ В ЮРИСПРУДЕНЦИИ

Аннотация. В статье изложены основные области, прямо или косвенно связанные с правовой действительностью, в которых применение кейлогеров, фиксирующих показатели компьютерного почерка человека, может принести значительную пользу. В качестве таковых обозначены: доказывание в суде, контроль и регулирование трудовых процессов, обеспечение личной информационной безопасности, защита персональных данных. В работе обосновываются достоинства технологии, а также обозначаются проблемные аспекты и возможные риски, связанные с широким распространением кейлогеров (предвзятое негативное отношение людей, потенциально возможные злоупотребления, риск нарушения баланса между свободой и безопасностью и т. д.). Основной целью статьи является привлечение внимания юридического сообщества к темам компьютерного почерка и кейлогеров, без чего распространение рассмотренной актуальной технологии представляется невозможным.

Ключевые слова: компьютерный почерк, кейлогер, процессуальное доказывание, трудовые отношения, контроль рабочего времени, информационная безопасность, двухфакторная аутентификация

SCOPE OF APPLICATION OF KEYLOGGER TECHNOLOGY IN JURISPRUDENCE

Abstract. The article outlines the main, in the author's opinion, scopes directly or indirectly related to the legal reality, in which the use of keyloggers, recording indicators of human keyboard's handwriting, can be of great benefit. These are court evidence, labour control and regulation, personal information security and personal data protection. The paper substantiates the merits of the technology, but also identifies the problematic aspects and possible risks associated with the widespread use of keyloggers (negative bias of people, potential abuse, risk of imbalance between freedom and security, etc.). The main purpose of the article is to draw attention of the legal community to the topics of computer handwriting and keyloggers, without which the dissemination of the considered topical technology seems impossible.

Keywords: Computer handwriting, Keylogger, Procedural evidence, Labour relations, Working time control, Information security, Two-factor authentication

Цифровые технологии стали неотъемлемой частью нашей жизни, порой мы даже не успеваем отследить новейшие достижения. В связи с этим неудивительно, что ряд технологий остаются вне правового поля, вне нормативного регулирования. Это может быть связано еще и с тем, что юриспруденция, зная о технологии,

считает ее неинтересной для себя, не видит возможных сфер применения. Иногда невнимательность и отсутствие интереса могут существовать одновременно. В настоящей работе мы осветим технологию кейлогеров, которую необоснованно, на наш взгляд, юристы обошли своим вниманием, о чем свидетельствует малое число научных работ по данной теме.

Кейлогеры, или перехватчики клавиатуры, – программы или аппаратные устройства, которые фиксируют показатели компьютерного почерка человека [9]. Последний представляет собой сложную систему печатно-двигательного навыка человека и хранящихся в его памяти образов ожидаемых символов, которая реализуется в процессе набора текста на клавиатуре. Компьютерный почерк индивидуален, воспроизводим и относительно устойчив. Он характеризуется следующими показателями.

1. Степень выработанности.

Характеристики степени выработанности компьютерного почерка

Степень выработанности	Число используемых пальцев	Скорость (зн/мин)	Число ошибок, %
Высокая	8–10	>200	<1,5
Средняя	3–8	100–200	1,5–5
Низкая	1–2	<100	>5

2. Темп печати – отвечает за время, затрачиваемое для набора единого смыслового элемента без отвлечения от процесса.

3. Скорость печати – показывает, сколько символов вводит исполнитель за единицу времени, учитывая и время, необходимое для формулирования мысли, проверки написанного и т. п.

4. Динамика ввода – описывает время, затрачиваемое на нажатие одной клавиши [2. С. 400].

5. Сила нажатия на клавиши.

6. Характер наложений – демонстрирует «зональность» клавиатуры, т. е. то, за какие области (клавиши), какие пальцы отвечают (рис. 1), происходит ли нажатие на очередную клавишу, когда предыдущая еще до конца не отпущена [8. С. 2].

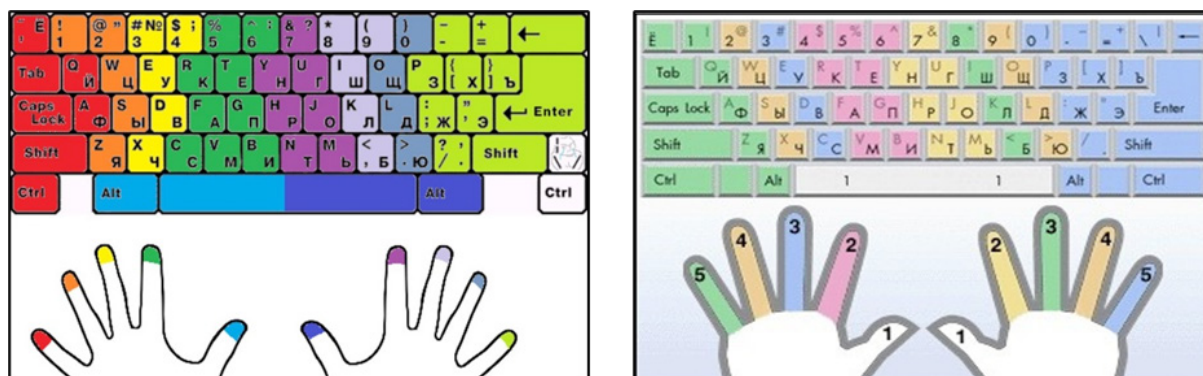


Рис. 1. Примеры возможных наложений

7. Системные опечатки – типичные для человека ошибки (например, пропуск буквы: «соответсвенно» вместо «соответственно»).

8. Модель внесения исправлений (см. рис. 2).



Рис. 2. Возможные модели внесения исправлений

9. Уровень компьютерной грамотности исполнителя – подразумевает использование служебных функций, горячих клавиш и т. п.

Все эти показатели способны зафиксировать кейлогеры. Программы-перехватчики устанавливаются на пользовательское устройство, обходя защиту антивирусов, и считывают описанные выше признаки, а также, в зависимости от настроек, запоминают посещенные сайты и запущенные программы. Далее они формируют отчет и направляют его по указанному в момент установки адресу электронной почты или по иным сетям связи. Аппаратные модули выглядят как небольшие флеш-накопители, которые подключаются к системному блоку либо самой клавиатуре. Принцип их работы аналогичен программам-перехватчикам

Кейлогеры – весьма известная технология в кругах программистов и лиц, профессионально занимающихся или просто интересующихся вопросами цифровой безопасности, однако, как указывалось выше, юристы знают о ней не так много. Это представляется не совсем корректным, потому что кейлогеры могут оказать неоценимую помощь населению и правоохранительной системе, если их ввести в правовое поле и практическую деятельность.

В первую очередь рассматриваемая технология позволяет установить исполнителя электронного сообщения или напечатанного документа [7. С. 113], что необходимо в процессе доказывания по уголовным, гражданским и арбитражным делам. Как указывалось в начале работы, компьютерный почерк индивидуален [6. С. 60], подделать его очень сложно – для этого нужно иметь представление о совокупности показателей, которые трудно фиксируются (например, скорость печати) или и вовсе не фиксируются (например, сила нажатия) человеческим глазом. Помимо этого, кейлогеры позволяют определить, на исследуемом ли оборудовании в действительности был напечатан текст или он был передан по зашифрованным каналам с подлогом IP-адреса и прочих идентификаторов компьютера.

Рассмотрим следующий пример. Лицо обвиняется в развращении несовершеннолетних на основании интернет-переписки. Проведенные компьютерно-технические экспертизы показали, что переписка велась с его компьютера; все стилистические особенности свидетельствуют об авторстве обвиняемого, однако он утверждает, что ничего подобного не писал. В этом случае, получив данные с предустановленного кейлогера, можно будет легко доказать, печатал ли человек на самом деле компрометирующий его текст или нет.

Мы упомянули здесь о предустановленном кейлогере, однако нигде выше не сказали, как это возможно. Следует отметить, что данный вопрос имеет ключевое значение: так, идентификационная экспертиза по определению исполнителя напечатанного текста и диагностические исследования, позволяющие сузить круг подозреваемых за счет определения возраста, эмоционального состояния, условий печати и т. п., будут возможны только в том случае, когда у экспертов на руках окажутся свободные образцы компьютерного почерка лица, выполнившего спорный текст. Данные образцы можно получить, только если на пользовательском оборудовании, где создавался текст, подлежащий экспертизе, заранее установлен кейлогер. Сейчас же ситуация такова, что большинство людей недоверчиво относятся к рассматриваемой технологии, поэтому редко можно найти человека, сознательно установившего кейлогер на свое устройство. Необходимо менять эту ситуацию.

Самым простым и одновременно недостижимым на практике является вариант повсеместного убеждения людей в том, что кейлогеры очень важны как средство предварительной защиты от потенциальных подлогов, надеясь, что население воспримет эту идею и станет широко использовать технологию. Однако на сегодняшний день у многих складывается впечатление, что данная технология несет в себе один только вред и угрожает безопасности [5].

Более правдоподобным представляется вариант с государственным вмешательством – государство обязует всех потребителей при покупке компьютерной техники устанавливать кейлогер или накладывает аналогичную обязанность на производителей, создавая в последнем случае единую государственную базу данных для получения отчетов абсолютно всех кейлогеров. Однако и эти предложения трудно реализуемы на практике: велика вероятность, что люди не захотят устанавливать кейлогеры, поэтому начнет процветать черный рынок компьютерной техники. Возложение же обязанности на производителей приведет к существенному удорожанию легальной компьютерной техники, что также спровоцирует рост незаконных сделок, а также может вызвать народное недовольство, аналогичное реакции на «Закон Яровой», что негативно скажется на популярности власти и, скорее всего, не позволит принять соответствующий закон. Помимо этого, остро встают вопросы информационной безопасности: где хранить массив данных о компьютерном почерке каждого гражданина (предполагаемый объем информации приведет к перегрузке серверов)? как избежать утечки персональных данных о компьютерном почерке населения? и др.

Наконец, есть третий вариант, при котором уже сейчас можно получить информацию о компьютерном почерке любого человека. Согласно данным, проверить

которые мы не имеем возможности в силу статуса, во всех компьютерах и ноутбуках изначально присутствует внедренный кейлоггер, который позволяет разработчикам программного обеспечения постоянно оптимизировать клавиатуры [10].

Таким образом, вопрос предустановленного кейлоггера еще предстоит решить и, чем больше людей заинтересуются технологией, осознав ее пользу, тем больше вероятность, что в скором времени мы сможем наблюдать рождение новой ветви судебных экспертиз по определению исполнителя напечатанного текста – задача, актуальность которой возрастает с каждым днем в условиях стремительно движущейся цифровизации и стратегии перехода всех государственных и рабочих процессов на электронный документооборот.

Далее, кейлоггеры могут применяться для контроля рабочего времени, трудовой активности и честности. Так, установив на рабочих устройствах кейлоггеры, работодатель сможет проследить, чтобы сотрудники соблюдали определенный порядок.

1. Приходили на работу в приемлемом состоянии и не перерабатывали (в тех сферах, где переутомление особенно опасно [3. С. 21–23], например в работе авиадиспетчера). Так, по изменениям компьютерного почерка, фиксируемым рассматриваемой технологией, можно установить, что человек устал, сильно волнуется, находится в состоянии алкогольного или иного опьянения. В таких ситуациях будут снижаться выработанность, увеличиваться число ошибок, замедляться темп и скорость и т. п.

2. Посвящали время работе, вместо того чтобы отвлекаться на игры и подобные посторонние активности. Так, работодатель имеет возможность с помощью кейлоггеров узнавать, какие сайты во время рабочего дня посещали сотрудники, какие приложения открывали, сколько времени реально исполняли свои трудовые обязанности, если они офисного формата, т. е. предполагают постоянный контакт с компьютером.

3. Добросовестно и самостоятельно выполняли порученные задания, а не воровали у коллег новаторские идеи. Этот аспект больше связан с творческими профессиями (дизайнер, менеджер по продажам и т. п.), где разработка нового проекта, идеи способна продвинуть по карьерной лестнице или гарантирует премию. В этом случае кейлоггеры, во-первых, позволят настроить возможность доступа к компьютеру либо отдельным файлам только того человека, который по почерку распознан как владелец, а во-вторых, дадут возможность доказать, что информацию по проекту с компьютера похитил коллега, так как разработки велись на данном устройстве, а не на компьютере недобросовестного сотрудника.

Однако, чтобы описанное выше стало возможным, необходимо, во-первых, законодательно предусмотреть возможность использования кейлоггеров для регулирования рабочих процессов и, во-вторых, обязать работодателя под угрозой юридической ответственности предупреждать работников и соискателей об этом – так как в противном случае будет иметь место незаконное получение сведений о личной жизни человека, незаконный доступ к его персональным данным. Разумным представляется на настоящем этапе оценить все возможные риски внедрения кейлоггеров в сферу трудовых отношений и начать только с критически важных отраслей, где промышленный шпионаж, невыполнение своих трудовых обязанностей и переутомление могут повлечь за собой крупный ущерб компании или вред обществу.

Наконец, кейлогеры могут оказаться полезными в криминологических целях предотвращения преступлений. Так, они позволяют настроить систему двухфакторной аутентификации, при которой доступ к компьютеру в целом или отдельным файлам, приложениям на нем становится возможным только в том случае, когда пароль введен человеком, признаки компьютерного почерка которого сохранены в системе [4]. Это позволит снизить риск хищений конфиденциальной информации, совершения противоправных или аморальных действий от имени владельца компьютера сторонним человеком и т. п. И именно данное направление применения кейлогеров видится нам наиболее приоритетным, поскольку, если люди осознают, что за счет данной технологии они могут защитить себя и свои секреты, они с большей вероятностью установят кейлогер на свое устройство, тем самым разрешив проблему получения впоследствии свободных образцов компьютерного почерка.

Таким образом, мы обозначили основные, наиболее заметные области юриспруденции, в которых вполне оправданным и даже очень полезным оказывается применение кейлогеров. Технологии не стоят на месте, цифровизация идет стремительными темпами, и юридическому сообществу следует, на наш взгляд, обратить внимание на кейлогеры, начав внедрять их в процессуальное доказывание, трудовые отношения и практику обеспечения личной информационной безопасности. Данная статья учитывает алгоритм исследования современных технологий методами юридической науки, согласно которому необходимо:

1. Изучить технологию, все ее возможности и ограничения.
2. Оценить риски внедрения технологии в практическую действительность.
3. Оценить общественное мнение относительно данной технологии, ожидания и опасения людей.
4. Подготовить этическую основу для внедряемой технологии.
5. Разработать правовые нормы, которые будут регулировать отношения, связанные с данной технологией [1. С. 28].

Исследование возможностей использования кейлогеров пока находится между вторым и третьим шагами указанного алгоритма. Для реализации дальнейших шагов представляется необходимым продолжать исследования, продвигаясь не только вперед, но и вглубь (собирать эмпирический материал, позволяющий установить точное отношение людей к кейлогерам и готовность общественности к появлению новой технологии; детальнее изучить риски и т. п.).

Список литературы

1. Бахтеев Д. В. Современные технологии как предмет изучения и инструмент в юридических исследованиях и юридической деятельности // Технологии XXI века в юриспруденции: материалы Второй международной научно-практической конференции, Екатеринбург, 22 мая 2020 г. / под ред. Д. В. Бахтеева. Екатеринбург: Уральский государственный юридический университет, 2020. С. 28.
2. Васильев В. И., Калямов М. Ф., Калямова Л. Ф. Идентификация пользователей по клавиатурному почерку с применением алгоритма регистрации частых биграмм // Моделирование, оптимизация и информационные технологии. 2018. Т. 6, № 1 (20). С. 399–407.

3. Васильев В. И., Сулавко А. Е., Борисов Р. В., Жумажанова С. С. Распознавание психофизиологических состояний пользователей на основе скрытого мониторинга действий в компьютерных системах // Искусственный интеллект и принятие решений. 2017. № 3. С. 21–37.

4. Как разработать систему, которая распознает человека по клавиатурному почерку // IDFinance. 27 апреля 2018. URL: <https://habr.com/ru/company/idfinance/blog/354492/> (дата обращения: 11.08.2022).

5. Клавиатурные шпионы, или Как клавиатура может предать вас // Новости мира IT. 11 октября 2019. URL: https://zen.yandex.ru/media/it_news/klaviaturnye-shpiony-ili-kak-klaviatura-mojet-predat-vas-5da04457ba281e00b3fa7a4d (дата обращения: 11.08.2022).

6. Перегудов А. В. Анализ клавиатурного почерка. Способы его применения // Interactive Science. 2018. № 6 (28). С. 60. URL: <https://elibrary.ru/item.asp?id=35125394>

7. Федоров И. З. К вопросу об установлении исполнителя электронного текста по клавиатурному почерку при раскрытии и расследовании преступлений // Вестник Барнаульского юридического института МВД России. 2019. № 2 (37). С. 114.

8. Algorithm for personal identification in distance learning system based on registration of keyboard rhythm / P. V. Nikitin, A. N. Savinov, R. I. Bazhenov, S. V. Sivandaev // Journal of Physics: Conference Series. 2018. № 1015, 042043. Pp. 1–5. URL: <https://iopscience.iop.org/article/10.1088/1742-6596/1015/4/042043/pdf>.

9. Cormac Herley, Dinei Florencio, Microsoft Research – How To Login From an Internet Cafe Without Worrying About Keyloggers // MSR-TR-2006-12. July 2006. URL: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/soups06.pdf> (дата обращения: 11.08.2022).

10. Where does Windows 10 save Keyboard input? URL: <https://security.stackexchange.com/questions/143322/where-does-windows-10-save-keyboard-input> (дата обращения: 11.08.2022).

С. Р. Чеджемов,

доктор педагогических наук, профессор кафедры
теории и истории государства и права,
Северо-Кавказский горно-металлургический институт
(государственный технологический университет);
Северо-Осетинская государственная медицинская академия

ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И ИНФОДЕМИЯ

Аннотация. В статье проводится анализ тенденций развития глобального информационного общества, в частности такое явление, как инфодемия, ее роль и значение в отношениях между странами и народами, в том числе и во внутренней политике государств. Этот своеобразный деструктивный идеологический вирус посредством компьютерных возможностей проник в современные общественные отношения и требует пристального интегрального анализа ученых

различных областей знания. Утверждается, что инфодемия уже сейчас активно используется в геополитической борьбе на фоне глобального экономического кризиса и усиления международной напряженности, поскольку ее последствия в значительной мере могут дестабилизировать общественно-политическую ситуацию в стране. В качестве одного из примеров в статье анализируется санитарно-гигиеническое требование ношения медицинских масок и перчаток и правовые последствия за его нарушение.

Ключевые слова: информационное общество, глобализация, инфодемия, санитария, международное право, правовые системы

INFORMATION PROCESSES AND INFODEMIA

Abstract. In the article, the problem of consideration is the analysis of trends in the development of the global information society, in particular such a phenomenon as infodemy, its role and importance in relations between countries and peoples, including in the domestic policy of states. This kind of destructive ideological virus through computer capabilities has penetrated into modern social relations and requires a close integral analysis of scientists in various fields of knowledge. The author believes that infodemy is already actively used in the geopolitical struggle against the background of the global economic crisis and increased international tensions, since its consequences can significantly destabilize the socio-political situation in the country. As one example, the article analyzes the sanitary and hygienic requirement to wear medical masks and gloves and the legal consequences for its violation.

Keywords: Information society, Globalization, Infodemy, Sanitation international law, Legal systems

Введение. Международно-правовые основы формирования информационного общества должны облегчить людям возможности коммуникаций, сделать более доступной и открытой информацию, а также облегчить информационный обмен между государствами. Возможность этого предусматривается и в нормах международного права, положения которого, согласно ст. 15 Конституции Российской Федерации, органически входят в правовую систему нашего государства.

Как известно, право на информацию было провозглашено в статье 19 Всеобщей декларации прав человека, в которой отмечалось: «Свобода и возможность получения и передачи информации являются основной потребностью и неотъемлемым правом каждого человека» [2]. Международным сообществом уделяется большое внимание вопросам правового регулирования использования Интернета, что и было закреплено в материалах специальной сессии Генеральной Ассамблеи ООН [3]. Однако ныне, в условиях различных вводимых санкций против нашей страны, ее руководства, да и граждан, многократно возрастает угроза применения возможностей Интернета, направленных на ослабление, а то и развал нашего государства.

Отрадно, что наше научное сообщество не стоит в стороне от решения злободневных задач в этом вопросе, и веским свидетельством этого стал настоящий форум. В России, по существу, создана научная школа, в центре исследования которой находится проблема информационного пространства, обеспечения информа-

ционной безопасности и взаимодействия различных фигурантов его обеспечения. Думается, что продуктивное исследование данной проблемы невозможно в рамках лишь юридических наук и требует взаимодействия с другими социально-гуманитарными науками в зависимости от того, какой вопрос выдвигается ученым в качестве объекта и предмета исследования. Только за последние годы этой проблеме был посвящен ряд работ отечественных ученых, изданных как на русском, так и на английском языках [7–19]. В работах процитированных авторов и некоторых других поднимаются важные проблемы общего спектра развития информационных технологий, но непосредственно инфодемии как таковой внимания почти не уделяется, хотя многие ее существенные характеристики исследуются. Быть может, эти авторы просто не приемлют данный термин. В настоящей статье мы попытаемся представить собственное видение этой проблемы, естественно, не претендуя на истину в этом вопросе.

Основная часть. Изменяются правовые стереотипы взаимоотношений между странами и народами, и это сопровождается синтезом технологий и их взаимодействием, в котором цифровизация становится не роскошью, а необходимым средством поступательного движения развития государства в деле обеспечения эффективной внутренней политики, одним из важнейших направлений которой является здравоохранение [7. С. 199–200]. Нам представляется, что, поскольку глобальные информационные процессы происходят в настоящее время с нарастающей быстротой, то появившееся на их фоне такое общественно значимое явление, как инфодемия, нуждается в оперативном специальном исследовании. Данный термин с легкой руки американского ученого Дэвида Роткопфома обозначает сочетание в едином целом устрашающих слухов по широкому спектру человеческой деятельности, в том числе и в сфере охраны здоровья. Инфодемия сегодня прочно обосновалась на современном информационном поле и охватила весь мир в период пандемии COVID-19 благодаря средствам массовой информации, в том числе социальным сетям – порождениям нашей современной информационной эры.

Инфодемия признана Всемирной организацией здравоохранения явлением общественной жизни, серьезно затрудняющим процесс борьбы с инфекционными заболеваниями [1]. Именно она стала основой так называемых протестных акций, затронувших Европу, да и весь мир. Здравоохранение неразрывно входит в общий спектр обеспечения безопасной жизнедеятельности, и этот сегмент научных исследований весьма удачно был интерпретирован на проходившем 22 декабря 2020 г. в Институте государства и права РАН научно-практическом форуме [13]. Профессор Т. А. Полякова справедливо отмечает усиление потребностей международного сообщества в объективной, достоверной и своевременной информации об общественных процессах [14. С. 20]. От себя добавим важность этой работы в системе общественного здоровья и санитарно-эпидемиологической безопасности населения.

Информация – важнейший ресурс современного человечества. Появившаяся новость привлекает внимание, прежде всего, своей актуальной значимостью. В этом плане вопросы здравоохранения, безопасности окружающей среды прочно лидируют в общественном сознании любого цивилизованного общества и государства. В этой работе велика роль средств массовой информации, в том числе электронных

[15. С. 237]. Какой тон по отношению к предписаниям государства они задают в обществе – аналитический, нейтральный, конформистский, враждебный?

Обратимся к некоторым вопросам, связанным с потрясшей мир пандемией COVID-19, тем более что, по мнению генерального директора Всемирной организации здравоохранения (ВОЗ) Тедроса Адана Гебрейесуса, «миру необходимо возвращаться к испытанным способам борьбы с COVID-19 в связи с ростом заболеваемости новыми штаммами коронавируса». Он заявил об этом в интервью британскому телеканалу Sky News и среди прочего призвал вновь носить маски [4]. Эта новость была мгновенно растиражирована, что вполне объяснимо с учетом ее значимости. В отечественных новостных лентах появилась информация о том, что «владельцы торговых центров, которые входят в Российский совет торговых центров (РСТЦ), пока не вернули обязательность ношения масок, но продумывают этот вопрос, рассказал РБК президент РСТЦ Дмитрий Москаленко. «Среди членов РСТЦ – “Корпорация А. Н. Д.” (Торговые центры “Смоленский пассаж”, “Калужский” и другие), “Ташир” (сеть торговых центров “Рио”, “Ереван Плаза”, Avenue South-West и другие), Ingka Centres (торговые центры “Мега”). В пресс-службе торгово-развлекательного комплекса “Остров мечты” рассказали РБК, что поддерживают меры эпидемической безопасности. В ближайшее время в ТРК начнут транслировать призывы для посетителей о ношении масок» [6].

Подобная информация вызвала и, думается, в еще большей степени вызовет определенные реакции среди мирового сообщества, а в общественном сознании породит немало домыслов и слухов. Они были и существуют в любом обществе на всем этапе его развития от примитивного до высокоорганизованного. Появление интернет-ресурсов в значительной мере облегчило создание и распространение слухов, что дало основание А. А. Кирзюку провести специальное исследование и на его основе выявить не только причины их появления, но и выделить категории людей, подверженных влиянию слухов и становящихся не только их объектами, но и субъектами» [11. С. 484].

Выделенная нами выше тональность электронных СМИ – аналитическая, нейтральная, конформистская, враждебная, конечно же, может считаться всеобъемлющей, есть и иные «оттенки», но в целом может служить основой для градации новостей, которые, в зависимости от тональности их подачи, причем не только вербальной, когда мы слышим голосовое сообщение, но и текстовой, во многом может как быть источником инфодемии, так и средством ее нейтрализации.

Совершенно правы наши отечественные ученые Н. В. Кроткова, А. В. Минбаев и Т. А. Полякова и некоторые другие, поднимающие вопрос о необходимости правового обеспечения информационной безопасности [9, 10, 12]. Вместе с тем опыт, хочется верить покинувшей нас, пандемии позволяет выявить и некоторые узкие места – огрехи как в законодательном, так и в правоприменительных сегментах.

В нашей работе мы попытаемся проанализировать это на примере таких средств профилактики, как медицинские маски и перчатки. Для большинства населения, даже прошедшего пандемию, они остаются, говоря словами из известного фильма «Формула любви», «предметом темным», и вот почему. Рекомендации по их ношению вызывали некоторые вопросы, например, та, с которой выступил Рособнадзор 10.04.2020. В ней говорилось: «Понимая, что новый коронавирус COVID-19 переда-

ется от человека к человеку либо воздушно-капельным путем, либо через контакт, ношение медицинской маски может выступать одной из профилактических мер для ограничения нового коронавируса» [5].

Эта информация о необходимости носить маски сразу вызвала волну обсуждений в интернет-сообществах, во время которых высказывались порой диаметрально противоположные мнения. В них затрагивался комплекс вопросов, на которые люди хотели получить категоричный ответ: Что говорит Всемирная организация здравоохранения о ношении масок? Кто должен обеспечивать пенсионера, работающего или учащегося масками? Должны ли жители городов и сел находиться на улицах в масках? и т. п.

И, если ответы на эти вопросы потребовали определенное, как нам кажется, не всегда оправданное время, то для прояснения ситуации на официальном сайте Роспотребнадзора была опубликована «Обновленная версия рекомендаций Всемирной организации здравоохранения по использованию масок в сообществах, во время ухода на дому и в медицинских учреждениях в контексте COVID-19», в которой говорилось следующее:

- «– аккуратно наденьте маску, чтобы полностью закрыть рот и нос, и надежно закрепите, чтобы минимизировать любые промежутки между лицом и маской;
- во время использования не касайтесь маски руками;
- снимите маску, используя соответствующую технику (т. е. не касайтесь передней части, а снимайте за шнурок сзади);
- после снятия или в случае непреднамеренного касания маски обработайте руки с помощью спиртосодержащего средства для мытья рук или мыла и воды, если они заметно загрязнены;
- меняйте маску на новую чистую, сухую, как только она становится влажной;
- не используйте повторно одноразовые маски;
- выбрасывайте одноразовые маски после каждого использования и утилизируйте их сразу после снятия».

Наряду с масками рекомендовалось под угрозой административного наказания и ношение перчаток. Мы попытались проанализировать практику вынесения наказаний за нарушение так называемого масочно-перчаточного режима. Серьезных академических исследований на этот счет нами пока обнаружено не было. Анализ разрозненной судебной практики требует определенного времени, поэтому можем лишь высказать собственную первоначальную точку зрения. За пределами этих инструкций осталось главное, на наш взгляд, невыясненное обстоятельство: какие маски считать «правильными» и не связано ли требование того, что тканевые (например, хлопковые или марлевые) маски не рекомендовались ни при каких обстоятельствах, с определенным коммерческим интересом.

Если призыв носить маски неоднократно звучал в средствах массовой информации, где и приводились конкретные случаи наказания за связанный с этим административный проступок, то ненаошение медицинских перчаток в целом оставалось «фигурой умолчания», т. е. это можно квалифицировать не как пробел в праве, а как своеобразное квалифицированное умолчание в действиях правоприменителя. Однако ни одного случая наказания за халатность компетентных сотрудников за ненадлежащий контроль за невыполнением предписания носить перчатки нами выявлено не было.

Следует также сказать, что в тех условиях социально незащищенные слои населения были поставлены перед необходимостью закупать маски и перчатки. Ситуацию подогрел и ажиотажный спрос на эти товары. Были мгновенно взвинчены цены.

Немало вопросов связано с обстоятельствами определения именно тех мест, где имели место вспышки заболеванием COVID-19. По стране поползли слухи о сокрытии информации на этот счет, причем власти упрекались одновременно и в занижении случаев заболевания, и в их увеличении. Нам представляется уместным позаимствовать опыт Министерства просвещения РФ, инициировавшего создание так называемого Совета учителей-блогеров, призванного обеспечить взаимодействие ведомства и учителей-блогеров в деле популяризации своей работы среди аудитории социальных сетей. Для регистрации желающих была помещена специальная ссылка.

Думается, что в медико-профилактической деятельности целесообразно создать аналогичный совет врачей-блогеров с целью привлечения внимания широких кругов общественности к нюансам здравоохранения, пропаганде здорового образа жизни и разоблачения явлений инфодемии. В данный совет было бы целесообразным включить и работников системы министерств юстиции, внутренних дел, науки и высшего образования.

Выводы. В современных условиях инфодемия будет все активнее использоваться в межгосударственном противостоянии, что становится одним из серьезных вызовов для информационной безопасности нашего государства, и требует соответствующей реакции с его стороны как внутри страны, так и среди международного сообщества.

Считаем, что информатизация общества во многом носит позитивный характер, так как способствует консолидации стран и народов в решении глобальных проблем, стоящих перед человечеством. Наряду с этим информационная глобализация сопряжена с рядом негативных явлений, одним из которых и является инфодемия. Для минимизации ее негативного влияния необходимо поднятие общего образовательного уровня населения и правовой культуры в частности. Представляется, что в этих целях необходимо повысить результативность сотрудничества населения, правоприменителей и информационных новостных и социальных средств. В этом важнейшее место должно отводиться единой государственной политике, поиску и внедрению новых средств и методов осмысления медико-профилактических мер и их широкой пропаганды в обществе.

Список литературы

1. ВОЗ. Инфодемия. URL: <https://zaim.com/glossary/ru-i/infodemiya/> (дата обращения: 07.11.2021).
2. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета. 1998. 10 декабря.
3. Генеральная Ассамблея ООН. Резолюции 74 сессии. URL: <https://www.un.org/ru/ga/74/docs/74res.shtml> (дата обращения: 27.06.2022).
4. Миру необходимо возвращаться к испытанным способам борьбы с COVID-19. URL: <https://tass.ru/> (дата обращения: 14.07.2022).

5. Об обновленной версии рекомендаций ВОЗ по использованию масок в сообществах, во время ухода на дому и в медицинских учреждениях в контексте COVID-19. URL: <https://www.rospotrebnadzor.ru/index.php> (дата обращения: 14.07.2022).
6. Российские торговые центры подготовились к возможному возвращению масок. URL: <https://news.mail.ru/society/5221372> (дата обращения: 16.07.2022).
7. Акопян Е. А., Акопян А. Р. Средства массовой информации, как социальный фактор формирования общественного мнения в современном обществе // Актуальные проблемы военно-научных исследований. 2021. № 2 (14). С. 237–246.
8. Александров А. С., Андреева О. И., Зайцев О. А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестник Томского государственного университета. 2019. № 448. С. 199–207.
9. Егорова М. А., Минбалеев А. В., Кожевина О. В., Дюфло А. Основные направления правового регулирования использования искусственного интеллекта в условиях пандемии // Вестник Санкт-Петербургского университета. Право. 2021. Т. 12, № 2. С. 250–262.
10. Полякова Т. А., Филатова Л. В. Влияние глобализации на построение информационного общества в России // Вестник РУДН. Серия: Информатизация образования. 2008. № 1. С. 20–26.
11. Кирзюк А. А. «У меня нет страха»: ковид-диссиденты в поисках агентности и правды // Мониторинг общественного мнения: экономические и социальные перемены. 2021. № 2. С. 484–509.
12. Кроткова Н. В., Минбалеев А. В., Полякова Т. А. Обзор Международной научно-практической конференции «Информационное пространство: обеспечение информационной безопасности и право» – Первые Бачиловские чтения // Государство и право. 2018. № 9. С. 138–148.
13. Материалы Международного научно-практического семинара «Векторы научных исследований правового регулирования обеспечения национальной и международной информационной безопасности в условиях больших вызовов и угроз». URL: <http://www.igpran.ru/konferentsii/programma-meropriyatii/7789/> (дата обращения: 11.07.2022).
14. Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Формирование системы информационного права как научного направления: этапы развития и перспективы // Государство и право. 2019. № 2. С. 80–92.
15. Чеджемов С. Р. Правовая культура россиян или уроки пандемии и инфодемии // История науки и техники. 2022. № 1. С. 12–20
16. Чеджемов С. Р., Золоева З. Т. Глобальное информационное общество – зло или благо человечества? // Государственная власть и местное самоуправление. 2022. № 7. С. 10–14.
17. Arkhipov V. V., Gracheva A. V., Naumov V. B., Polyakova T. A., Minbaleev A. V. Definition of artificial intelligence in the context of the russian legal system: a critical approach // State and Law. 2022. № 1. С. 168–178.
18. Bundin M., Martynov A., Minbaleev A. Legal aspects of the use of biometric students' identification for distant and online learning: Russian perspective // ACM International Conference Proceeding Series. 22, Digital Innovations for Public Values: Inclusive Collaboration and Community. Ser. "Proceedings of the 22nd Annual International

Conference on Digital Government Research: Digital Innovations for Public Values: Inclusive Collaboration and Community, DGO 2021”. 2021. Pp. 564–566.

19. Zhernova V. M., Minbaleev A. V. The integrated regulation of a cyber-physical system // CEUR Workshop Proceedings. Ser. “AISI 2021 – Proceedings of the International Workshop on Advances in Information Systems, Mathematical Modeling, and IT Applications in Industry”. 2021. Pp. 116–124.

Е. А. Честнов,

студент,

Московская академия Следственного комитета Российской Федерации

К. Т. Цветков,

студент,

Московская академия Следственного комитета Российской Федерации

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ВЕБ-АРХИВОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С РАСПРОСТРАНЕНИЕМ НЕГАТИВНОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ

Аннотация. В статье рассмотрены возможности использования ресурсов «Веб-архив» при производстве следственных и иных процессуальных действий в рамках расследования преступлений, связанных с распространением так называемого негативного контента и совершенных с использованием информационно-телекоммуникационных сетей. Проанализирована практика использования веб-архивов в качестве доказательства с точки зрения межотраслевого подхода (в рамках арбитражного и гражданского судопроизводства), а также перспективы использования данного метода в сфере уголовного судопроизводства, в частности, предварительного расследования.

Ключевые слова: негативный контент, следователь, цифровые следы, веб-архив, скриншот, следственные действия, специалист, криминалистическая техника

THE POSSIBILITY OF USING WEB ARCHIVES IN THE INVESTIGATIONS OF CRIMES RELATED TO THE DISTRIBUTION OF NEGATIVE CONTENT ON THE INTERNET

Abstract. The article discusses the possibilities of using the resources of the “Web Archive” in the production of investigative and other procedural actions in the investigation of crimes related to the distribution of so-called “negative content” and committed using information and telecommunications networks. The article considers the practice of using web archives as evidence from the point of view of an intersectoral approach (in the framework of arbitration and civil proceedings), as well as the prospects of using this method in the field of criminal proceedings, and in particular – preliminary investigation.

Keywords: Negative content, Investigator, Digital traces, Web archive, screenshot, Investigative actions, Specialist, Forensic equipment

В современном мире динамично развиваются информационные технологии и те виды преступной деятельности, которые еще 20–30 лет назад предполагали тщательную подготовку и планирование со стороны злоумышленников, а сегодня увеличенными темпами осуществляются в виртуальном пространстве. Сеть Интернет, наряду с, безусловно, положительными аспектами, привнесла в нашу действительность широкий спектр возможностей для совершения и сокрытия преступлений. По большей части это затронуло преступления, связанные с распространением так называемого негативного контента, которые в настоящее время представляет серьезную угрозу интересам государства и общества, охраняемым уголовным законом. К преступлениям, связанным с распространением так называемого негативного контента можно отнести составы преступлений, предусмотренные статьями 110.2, 135, 212, 282, 354.1 Уголовного кодекса Российской Федерации (далее – УК РФ), а также иные. Стоит отметить, что перечень составов преступлений, содержащих в себе в качестве признака объективной стороны действия, направленные на распространение негативного контента, постоянно дополняется законодателем. Так, в последнее время повысилась преступная активности в Интернете, связанная с участвовавшими случаями дискредитации Вооруженных сил Российской Федерации в контексте проведения специальной военной операции на Украине. Законодатель довольно быстро отреагировал на эти обстоятельства, и в Кодекс Российской Федерации об административных правонарушениях был внесен состав соответствующего правонарушения, а также в УК РФ был внесен аналогичный состав преступления, содержащий административную преюдицию.

Как правило, негативный контент выражается либо в текстовых сообщениях на веб-страницах, либо в форме изображения или видеофайла. Они и являются основным материалом, на основе которого следователь при производстве проверки сообщения о преступлении сможет сделать вывод о наличии признаков того или иного преступления, совершенного с использованием информационно-телекоммуникационных сетей, либо в рамках уже возбужденного уголовного дела получить потенциальную доказательственную базу. Видеофайл, набранный машинописный текст, графическое изображение – все эти данные и являются составляющими негативного контента, т. е. цифровыми следами преступления, соответственно, они подлежат фиксации и изъятию, а в последующем и процессуальному оформлению.

Как известно, обнаружение цифровых следов преступлений, оставленных, к примеру, в социальных сетях и (или) мессенджерах, относится к поисковой деятельности следователя, которая направлена на собирание доказательственной и ориентирующей криминалистически значимой информации [4. С. 108]. Поскольку такие следы быстро трансформируются и легко уничтожаются, промедление или неосторожные действия при их выявлении в ходе производства следственных действий могут привести к необратимым последствиям [1. С. 41]. На практике указанные условия создают определенные трудности при их обнаружении, изъятии, фиксации и документировании.

В сравнении с другими видами следов цифровые следы преступления зачастую подвержены сокрытию со стороны виновного лица, так как для уничтожения

определенной текстовой информации, изображения или видеофайла, как правило, достаточно нажатия одной клавиши или выполнения одной программной команды, буквально за несколько секунд возможно уничтожить большое количество доказательно важной информации. Данные обстоятельства могут создать широкие возможности для противодействия расследованию.

В настоящее время широко распространены интернет-сервисы, которые используют специальную технологию поисковых роботов, которые перебирают страницы сети Интернет и заносят информацию о них в свои базы данных, тем самым архивируя ее. Таким образом, благодаря общедоступности и обширной накопленной базе данных сервисы по просмотру архивных копий веб-страниц пользуются популярностью. Самым крупным подобным ресурсом является «WayBack Machine» – используя данный веб-инструмент, можно просмотреть практически любую страницу в Интернете в том виде, в котором она существовала в заданное пользователем время. Стоит отметить, что в настоящее время появился также и отечественный ресурс «Веб-архив.ру».

Вышеуказанные инструменты могут оказать значительную помощь следователю в преодолении противодействия предварительному расследованию, выражающемуся в уничтожении виновным лицом информации, имеющей доказательственное значение, в частности и информации, содержащей признаки так негативного контента. Однако процессуальный порядок использования подобных инструментов законодателем не уточнен, к тому же в ходе прохождения практики в качестве общественного помощника следователя в управлении криминалистики ГСУ СК России по Московской области было проведено интервьюирование сотрудников, в ходе которого четыре из четырех опрошенных следователей-криминалистов пояснили, что данные ресурсы в следственной практике не используются. Судебная практика по уголовным делам, где в качестве допустимого доказательства фигурировали бы данные, полученные посредством веб-архивов, в исследуемых источниках также отсутствует.

Стоит отметить, что в рамках арбитражного и гражданского судопроизводства уже достаточно давно существует практика использования информации из веб-архивов в качестве доказательства. Так, Арбитражный суд города Москвы в своем Решении от 17 июля 2017 г. по делу № А40-206553/2015 указал следующую характеристику рассматриваемого сервиса: «Доказательства, представленные Истцом с сайта <https://archive.org/web>, являются допустимыми и относимыми». Схожая позиция просматривается также и в иных судебных решениях. Также использование приведенного сайта при доказывании рекомендовано федеральными государственными органами, в частности Федеральной антимонопольной службой России в Письме от 28.08.2015 № АК/45828/15 «О рекламе в сети «Интернет», что означает, что данному ресурсу можно доверять в части предоставления им информации.

Использованию веб-архивов в качестве доказательства посвящены и работы ученых в области арбитражного процесса, так, А. И. Савельев справедливо отмечает: «Консерватизм, проявляемый судами при оценке допустимости тех или иных доказательств, полученных из сети Интернет, дополнительно осложняет положение потерпевшей стороны при попытках защиты ее прав, нарушенных действиями в сети

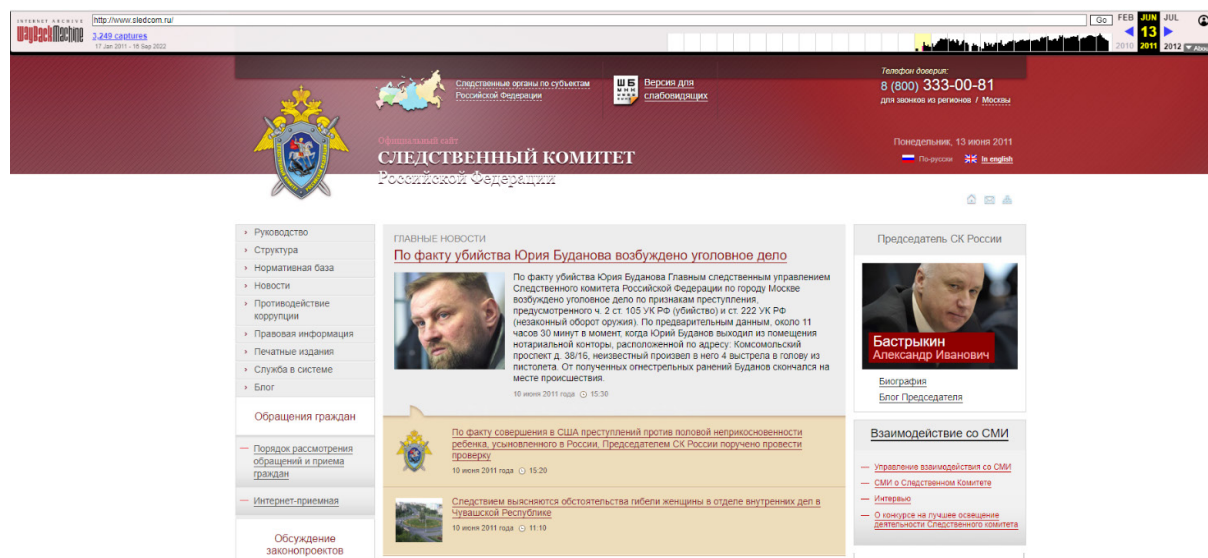
Интернет. Все это создает неоправданные преимущества для недобросовестных лиц. В то же время существуют определенные ресурсы, позволяющие продемонстрировать, как выглядела та или иная интернет-страница в определенный момент времени, даже если она впоследствии была удалена или изменена [5. С. 80–96]».

При этом применительно к процессу расследования преступлений хотелось бы отметить, что в современных условиях расследование преступлений связанных с распространением негативного контента, в том числе связанных с организацией, склонением и призывами к массовым беспорядкам, осложняется также тем, что их организация, содействие таковым и непосредственное осуществление нередко связаны с преступной деятельностью экстремистских и террористических сообществ и организаций, и прежде всего, с распространением ими соответствующей идеологии и активным использованием для этого широких возможностей Интернета и других информационно-коммуникационных технологий, на что также обращено внимание в Стратегии национальной безопасности Российской Федерации. Более того, в связи с проходящей в данный момент специальной военной операцией, а также участвовавшими случаями дискредитации Вооруженных сил Российской Федерации в сети Интернет рассматриваемые положения являются наиболее актуальными. Количество уголовных дел данной категории растет, соответственно, расследование необходимо проводить в максимально короткие сроки.

Наметилась устойчивая тенденция активного использования широких возможностей информационно-коммуникационных технологий для распространения различных материалов экстремистского содержания, а также для дискредитации Вооруженных сил Российской Федерации в Интернете. Из всего этого следует, что при подготовке и совершении преступлений в Сети преступники активно используют форумы, социальные сети, мобильную связь и другие возможности в условиях развития информационных технологий. Особое значение для раскрытия и расследования преступлений, связанных с распространением негативного контента, имеет работа с цифровыми следами.

Как уже отмечалось, цифровые следы зачастую подлежат сокрытию и уничтожению виновным лицом. При работе по сбору такого рода доказательств следователь может самостоятельно использовать возможности криминалистической техники и/или помощь специалистов для восстановления удаленного контента, а также направить запрос интернет-провайдеру и, приложив соответствующее судебное разрешение, истребовать необходимую информацию (к примеру, если речь идет о интернет-переписке). Однако все указанные действия требуют времени и нередко связаны с организационными издержками, такими как необходимость принимать меры по привлечению к участию в следственном действии соответствующего специалиста либо к доставлению на место производства следственного действия криминалистической техники. С другой стороны, для того чтобы в ходе расследования использовать веб-архив, не требуется специальных знаний и криминалистической техники, что позволяет существенно ускорить производство следственного действия, а вместе с этим и расследование в целом. Тем самым использование открытых возможностей Интернета позволяет в кратчайшие сроки получить необходимую информацию. Данные сервисы позволяют просматривать архивные

копий веб-страниц за определенный промежуток времени (рис.), в том числе те записи, которые на момент определенной даты еще не были удалены и история данных сообщений была сохранена в базе данных ресурса. Применять функции веб-архива Wayback Machine и «Веб-архив.ру» можно как на сайтах различных сетевых форумов, так и в социальных сетях («ВКонтакте», «Одноклассники» и др.), которые нередко используются для размещения негативного контента.



Пример работы с веб-архивом Wayback Machine. Открыта главная страница официального сайта Следственного комитета Российской Федерации по состоянию на 13 июня 2011 г.

Представляется, что фиксировать и исследовать следы так называемой интернет-активности необходимо с помощью оформления соответствующего протокола осмотра. В данном протоколе необходимо указывать на условия и порядок использования функции соответствующего веб-архива, находящегося в открытом доступе в Интернете, в частности, информацию о том, к какой именно веб-странице и за какой промежуток времени применялись возможности веб-архива. Далее в протоколе указывается информация о средствах фиксации полученных данных. Как правило, информация фиксируется при помощи создания снимка экрана устройства (скриншота) [2. С. 376–379; 3. С. 128–133], на котором содержится информация, представляющая интерес для следствия. На завершающем этапе осмотра изображения целесообразно распечатать на листах формата А4, после чего составить фототаблицу с соответствующим содержанием. В целях принятия дополнительных мер по обеспечению сохранности доказательств возможна также и запись скриншотов на физический носитель (компакт-диск или флеш-карту), который должен быть упакован способом, исключающим несанкционированный доступ, скреплен подписями участвующих лиц и печатью, после чего приобщен к протоколу следственного действия.

В целом отсутствуют какие-либо препятствия к использованию веб-архивов в качестве доказательства в уголовном судопроизводстве. Умелое использование

возможностей веб-архива помогает получить нужные для следователя сведения, которые могут быть в дальнейшем использованы для доказывания события преступления, а также мотива и цели. Как было отмечено, практика использования данных интернет-ресурсов в гражданском и арбитражном процессе уже имеется и широко используется в доказывании по соответствующим судебным делам. Представляется, что данная тенденция может затронуть и сферу уголовного судопроизводства, однако для формирования устойчивой судебной практики необходимо внедрять в следственную практику способы обнаружения, изъятия и фиксации потенциально новых видов следов преступления, с тем чтобы в последующем придать им правовой статус допустимого доказательства.

Все это свидетельствует о том, что развитие информационно-телекоммуникационных технологий непосредственным образом влияет на тактику следственных действий и методику расследования преступлений, связанных с распространением негативного контента. Представляется, что возможности использования открытых интернет-ресурсов в целях расследования преступлений на практике явно недооценены.

Список литературы

1. Галимханов А. Б., Халиуллина А. Ф. Порядок обнаружения, фиксации и изъятия цифровых следов преступления // Правовое государство: теория и практика. 2020. № 4–2 (62). URL: <https://cyberleninka.ru/article/n/poryadok-obnaruzheniyaizyatiya-i-fiksatsii-tsifrovyyh-sledov-prestupleniya> (дата обращения: 15.09.2022).

2. Лебедева А. А. Расследование киберпреступлений следователями СК России // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции: сборник материалов I Всероссийской научно-практической конференции. Москва, 27 января 2021 г. Москва: Университет прокуратуры Российской Федерации, 2021. С. 376–379.

3. Лебедева А. А. Тактика использования screenshot в доказывании по уголовным делам // Высокотехнологичное право: генезис и перспективы: материалы III Международной межвузовской научно-практической конференции. Москва – Красноярск, 24–25 февраля 2022 г. Красноярск: Красноярский государственный аграрный университет, 2022. С. 128–133.

4. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). URL: <https://cyberleninka.ru/article/n/problemy-sobiraniyatsifrovyyh-sledov-prestupleniy-iz-sotsialnyh-setey-i-messendzherov> (дата обращения: 15.09.2022).

5. Савельев А. И. Использование материалов интернет-архива Wayback Machine в качестве доказательства в арбитражном процессе // Вестник Высшего Арбитражного Суда Российской Федерации. 2013. № 12. С. 80–96.

В. А. Чукреевкандидат юридических наук,
прокуратура Свердловской области, заместитель прокурора**СПОРНЫЕ ВОПРОСЫ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ ОБОРОТА
ПОРНОГРАФИЧЕСКИХ МАТЕРИАЛОВ В ВИРТУАЛЬНОМ
ПРОСТРАНСТВЕ: РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ**

Аннотация. Целью работы является исследование проблем уголовной ответственности за оборот порнографической продукции в российском и зарубежном праве. В статье проводится анализ предмета и объективных признаков рассматриваемой группы преступлений, вопросы правовой оценки обращения порнографических материалов в виртуальном пространстве в российском и зарубежном праве, рассматриваются правовые подходы к их квалификации. В результате проведенного исследования были сделаны выводы о целесообразности внесения в уголовное законодательство изменений, позволяющих устранить имеющиеся законодательные противоречия и пробелы.

Ключевые слова: порнографические материалы, виртуальное пространство, частная жизнь, сексуальные посягательства, шантаж

**CONTROVERSIAL ISSUES OF CRIMINAL AND LEGAL ASSESSMENT
OF THE TURNOVER OF PORNOGRAPHIC MATERIALS IN THE VIRTUAL
INDUSTRY: RUSSIAN AND FOREIGN EXPERIENCE**

Abstract. The purpose of this article is to investigate the issues of criminal liability for trafficking in pornographic materials in Russian and foreign law. The article analyzes the subject matter and objective characteristics of the considered group of crimes, issues of legal assessment of the turnover of pornographic materials in virtual space in Russian and foreign law, and examines legal approaches to their qualification. As a result of the study, conclusions were made on the expediency of introducing amendments to the criminal law, allowing to eliminate existing legislative contradictions and gaps.

Keywords: Pornographic materials, Virtual space, Privacy, Sexual assaul, Blackmail

В многочисленных исследованиях современного состояния контента в сети Интернет приводятся различные данные об объеме порно-трафика. Иногда различие достаточно впечатляющие. По данным одних специалистов в 2015 г. общее количество поисковых запросов превысило два млрд из них 20 % относились к порнографии. По мнению Internet Safety-101 порядка 30 % всего видео-контента представляют собой порноматериалы, третья группа исследователей полагает, что порнография занимает нишу не более, чем в 10 % Сети, а сайты, содержащие сцены сексуального характера не превышают 4 % [1]. Несмотря на различия в исследовательских материалах, проблема широкого распространения порнографии в виртуальном пространстве совершенно очевидна. Правоприменители реагируют на подобные действия в рамках уголовного законодательства, однако и их позиции не всегда совпадают. Во всяком случае, единого понимания применяемых в уголовном законодательстве терминов пока не прослеживается.

В России, в отличие от многих других стран, законодателем или судом общего определения порнографии, которое применимо к уголовным делам, возбуждаемым по ст. 242 УК РФ, не предложено. Однако было разработано несколько законопроектов, ограничивающих оборот порнографической продукции, в одном из которых в ст. 2 порнография определялась как детализированное, натуралистическое изображение, словесное описание или демонстрация полового акта, половых органов, имеющие целью сексуальное возбуждение [2. С. 349].

В судебной практике в отдельных делах суды указывают на признаки, которые, по их мнению, присущи порнографии. Так, в одном из судебных решений подчеркнуто, что сексуальные сцены детализированы с фиксацией внимания на половых органах и ощущениях действующих лиц, с использованием крупного плана, специальных ракурсов, приемов и освещения при показе половых актов, подчеркивающих физиологические и анатомические детали [3].

Определение, данное в примечании 1 ст. 242.1 УК РФ относится к детской порнографии и имеет свою специфику. Под детской порнографией понимают материалы и предметы, содержащие любое изображение или описание в сексуальных целях: полностью или частично обнаженных половых органов несовершеннолетнего; несовершеннолетнего, совершающего либо имитирующего половое сношение или иные действия сексуального характера; полового сношения или иных действий сексуального характера, совершаемых в отношении несовершеннолетнего или с его участием; совершеннолетнего лица, изображающего несовершеннолетнего, совершающего либо имитирующего половое сношение или иные действия сексуального характера.

В целом данное определение соответствует по своему уровню, принятым в зарубежном законодательстве и международном праве дефинициям порнографии. Так, Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии от 25 мая 2000 г. подтверждает запрет на детскую порнографию, определяя последнюю как «любое изображение какими бы то ни было средствами ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка главным образом в сексуальных целях» (ст. 2 Протокола) [3].

В законодательном определении в ст. 242.1 УК РФ предлагается рассматривать детскую порнографию как в тех случаях, когда в качестве статиста в ее изготовление вовлечен несовершеннолетний, так и в ситуации, когда ребенка изображает взрослый статист. В то же время, с учетом современных возможностей компьютерной графики нередко встречаются хорошо смоделированные ситуации, в которых человек вообще участия не принимает, но изображение ребенка, между тем, сделано очень правдоподобно. Нередко изготовители порнографической продукции используют в таких целях образ реального несовершеннолетнего. Как представляется, в таких случаях также следует рассматривать смоделированный сюжет как детскую порнографию, однако, исходя из легального ее определения, предмет преступления, предусмотренного ст. 242.1 УК РФ в этой ситуации отсутствует. Однако этот пробел целесообразно устранить, поскольку объект преступления, присущий обращению детской порнографии нарушается и в данном случае.

Объективная сторона оборота порнографической продукции состоит из ряда действий, в том числе рекламирования, распространения, публичной демонстрации.

Наибольшее число сложностей вызывает правовая оценка распространения порнографии в сети Интернет.

В теории уголовного права распространение порнографии понимается как выполнение действий, в результате которых порнографические материалы могут быть использованы другими лицами. Такие действия заключаются в непосредственном предоставлении порнографической информации потребителю или могут проявляться в виде направления потребителю ссылки, используя которую пользователь получает доступ к нужной информации [4. С. 38–41].

Еще один взгляд на эту проблему связан с пониманием распространения как передачи любым способом как возмездно, так и безвозмездно, соответствующих предметов (носителей информации) [5. С. 130–131].

Применительно к виртуальному пространству такой вариант понятия термина «распространение» должен быть связан с активной деятельностью, с предложениями передать порнографическую информацию другим людям, конкретно определенным.

Ранее приведенное определение рассматриваемого признака позволяет предположить, что распространение порнографии допустимо также среди неопределенного круга лиц, причем как путем действия, так и путем бездействия. Соглашаясь с тем, что распространение запрещенного контента как признак преступления, предусмотренного ст. 242.1 УК РФ, имеет место при направлении предмета как одному конкретному лицу, так и неопределенному кругу лиц, позволю не согласиться с тем, что этот вид преступной деятельности может быть выполнен путем бездействия. Лицо, распространяющее информацию, согласно словарю С. И. Ожегова целенаправленно делает ее доступной, известной для многих. Для этого оно должно активно действовать.

В настоящее время вопрос о том, должен ли распространитель информации действовать активно или это не обязательно для признания в его поведении признаков объективной стороны ст. 242.1 УК РФ, связан с увеличением числа дел, в которых запрещенная информация становится доступной другим лицам путем использования пиринговых файлообменных сетей.

В большинстве уголовных дел суды признают сам факт размещения видеофайлов с порнографическим изображением несовершеннолетних в папках в персональном компьютере или на страницах сайта, доступных для просмотра и копирования другими пользователями, распространением информации. Однако однозначной позиции по этому вопросу судебная практика не выработала.

Так, К. был осужден за то, что, будучи пользователем страницы интернет-сайта, незаконно распространил доступный для просмотра и копирования другими пользователями указанного сайта видеофайл, являющийся порнографическим материалом, к которому обратились не менее десяти пользователей сети Интернет. Из материалов дела не ясно, предлагались ли данные порнографические материалы другим лицам или они сами инициативно разыскивали подобный контент на страницах интернет-сайта. Тем не менее К. был осужден за распространение порнографических материалов с изображением несовершеннолетних, не достигших 14 лет [6].

Вместе с тем подобная позиция районных судов не всегда находит поддержку вышестоящих инстанций. Рассмотрим следующий пример.

Таким образом, исходя из приведенного определения, можно сделать вывод, что распространение порнографических материалов Верховный Суд РФ связывает с целенаправленной деятельностью субъекта, проявляющейся в предложении и передаче запрещенного контента отдельным лицам. Эта позиция представляется вполне обоснованной, исходя из того, что противоправное поведение субъекта, согласно закону, должно характеризоваться прямым умыслом, т. е. субъект осознает, что он именно распространяет порнографические материалы (а не предоставляет возможность ознакомиться с ними неопределенному кругу лиц) и желает эти действия совершить.

В зарубежном законодательстве распространение детской порнографии рассматривается как серьезное нарушение закона. Так, в США глава 71 Title 18 USC «О непристойности» содержит перечень запрещенного поведения, связанного с оборотом порнографической продукции в виртуальном пространстве.

Разумеется, двумя этими статьями не исчерпывается огромный блок преступлений, сопряженных с детской порнографией, содержащейся в американском федеральном уголовном законодательстве. Однако некоторые аспекты защиты детей от рассматриваемых посягательств можно было принять во внимание и российскому законодателю. В частности, уточнить понятие детской порнографии, включив в него запрет на обращение визуальных произведений, смоделированных с помощью специального программного обеспечения без участия несовершеннолетних статистов.

В рамках правоприменения, было бы целесообразно оценивать распространение порнографических материалов в виртуальном пространстве как целенаправленную деятельность, проявляющуюся в предложении, адресованном конкретным лицам или неопределенному кругу лиц, передать порнографические материалы для самостоятельного их использования.

Список литературы

1. Семина Н., Фомина В. Каков на самом деле объем порнографии в сети Интернет? URL: // <https://intrigue.dating/> (дата обращения: 15.08.2022).
2. Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дисс. ... д-ра юрид. наук, Москва, 2015. 607 с.
3. Конвенция о правах ребенка (принята и открыта для подписания, ратификации и присоединения Резолюцией № 44/25 Генеральной Ассамблеи ООН от 20 ноября 1989 г.) // Международные акты о правах человека: сб. док. – Москва, 2000.
4. Джинджолия Р. С. Порнография. Уголовно-правовая характеристика. М, 2005. – 65 с.
5. Заирная М. М. Преступления в сфере оборота порнографических материалов и предметов: дисс. ... канд. юрид. наук. Москва, 2016. 213 с.
6. Дело № 10–97/10//<https://rospravosudie.com/court-volzhskiigorodskoj-sud-volgohradskaya-oblast-s/act-101306925/> (дата обращения: 27.08.2022).

Е. И. Шевалдина,

кандидат социологических наук, доцент,
Уфимский государственный нефтяной технический университет

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ КОНТРОЛЯ ЗА БЕЗНАДЗОРНЫМИ ЖИВОТНЫМИ

Аннотация. В данной статье рассматриваются вопросы обращения с безнадзорными животными, проводится анализ новейших технологических решений в сфере контроля животных, оставшихся без владельцев. Изучаются перспективы применения технологии распознавания животных, как одного из самых перспективных и инновационных направлений в рамках реализации информационно-аналитической системы «ЗОО-защита». Рассмотрены основные характеристики, преимущества и перспективы применения данной системы.

Ключевые слова: цифровая платформа работы с безнадзорными животными, информационно-аналитическая система «ЗОО-защита», распознавание животных

IMPROVEMENT OF THE INFORMATION AND ANALYTICAL CONTROL SYSTEM FOR NEGLECTED ANIMALS

Abstract. This article discusses the treatment of neglected animals, analyzes the latest technological solutions in the field of control of animals left without owners. The prospects of using animal recognition technology as one of the most promising and innovative directions in the implementation of the information and analytical system “ZOO-protection” are being studied. The main characteristics, advantages and prospects of application of this system are considered.

Keywords: a Digital platform for working with neglected animals, Information and analytical system “ZOO-protection”, Animal recognition

Федеральный закон от 27.12.2018 № 498-ФЗ «Об ответственном обращении с животными и о внесении изменений в отдельные законодательные акты Российской Федерации» (с учетом изменений, внесенных Федеральным законом от 14.07.2022 № 269-ФЗ) призван урегулировать отношения в области обращения с животными в целях защиты животных, а также укрепить основы нравственности, обеспечить соблюдение принципов гуманности, безопасности и иных прав и законных интересов граждан при обращении с животными [3]. Среди основных принципов документа – «отношение к животным, как к существам, способным испытывать эмоции и физические страдания», и «воспитание у населения нравственного и гуманного отношения к животным».

Статья 18 Федерального закона от 27.12.2018 № 498-ФЗ «Организация мероприятий при осуществлении деятельности по обращению с животными без владельцев» гласит, что «...мероприятия при осуществлении деятельности по обращению с животными без владельцев включают в себя в том числе отлов животных без владельцев, их транспортировку и немедленную передачу в приюты для животных».

Исполнителями мероприятий при осуществлении деятельности по обращению с животными без владельцев на территории муниципалитетов могут привле-

каться юридические лица и индивидуальные предприниматели в соответствии с требованиями, предусмотренными законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд. Отлов животных без владельцев должен производиться данными юридическими лицами и индивидуальными предпринимателями на основании принятых органом местного самоуправления подзаконных актов, определяющих порядок данной деятельности.

Выделяются огромные средства из государственного бюджета на процесс ОСВВ (отлов – стерилизация – вакцинация – возврат), но в итоге спросить оказывается не с кого, и, чаще всего, дела о нападениях бродячих животных на людей заканчиваются в судах. Программа ОСВВ выполняется недобросовестно и отследить качество работы невозможно, на обращения граждан в государственные и муниципальные службы по телефону не реагируют, у частных приютов нет финансирования, они живут за счет пожертвований населения.

В Республике Башкортостан за I полугодие 2022 г. за антирабической помощью обратилось 4 495 человек, показатель обращаемости 112,0 на 100 тыс. населения, что ниже среднемноголетнего уровня в 1,2 раза (129,1 на 100 тыс. населения). От собак получили повреждения 2 924 человек (65 % всех обратившихся). От диких животных получили ранения 15 человек. Остается на высоком уровне обращаемость детей за медицинской помощью от нападений животных – 1 353 человек (30,1 %). При этом 74,3 % повреждений получены от собак [1].

Причина такой ситуации объясняется отсутствием системного подхода к контролю за безнадзорностью животных. До настоящего времени нет алгоритмов и технологий выявления мест скопления животных без владельцев, передаче заявок в специализированные организации на отлов, юридического сопровождения процесса.

В рамках национальной программы «Цифровая экономика Российской Федерации» была предложена к реализации инновационная цифровая платформа, способная повысить эффективность работы частных и государственных служб, задействованных в сфере решения проблем безнадзорных животных, привлечь более широкий круг социально-активного населения, значительно расширить освещение проблематики для граждан России и реализовать гуманные методы уменьшения численности бродячих животных на улицах наших городов [2]. Однако эта цифровая платформа не решает проблем выявления мест и маршрутов миграции животных без владельцев на территории муниципалитетов.

С целью решения данной проблемы могут быть использованы разрабатываемые в настоящее время технологии распознавания животных – одно из самых перспективных и инновационных направлений в рамках реализации информационно-аналитической системы «ЗОО-защита» (далее – ИАС). Распознавание животных, особенно безнадзорных собак, – это практическое приложение теории распознавания образов, в задачу которого входит автоматическая локация животных в видеопотоке, состоящем из более 500 контрольных точек. Алгоритмы системы способны распознавать животных с хозяином и без хозяина, чипованных и нечипованных животных, вести учет животных на выбранной территории, формировать маршрут движения отдельных особей и стай по территории населенного пункта, направлять предупреждения об опасности жителям и специальным службам в виде СМС или push уведомлений при появлении собак на контрольной тер-

ритории. Система способна контролировать условия выгула домашних животных в соответствии с законом. Возможно использование ИАС совместно с системами автоматической рассылки штрафов гражданам, нарушающим правила выгула своих питомцев. Преимущества данной системы в том, что работа системы построена на штатном оборудовании, серверах, коммутаторах и камерах наружного наблюдения, установленных во всех городах и населенных пунктах Российской Федерации. ИАС работает в сложных погодных условиях, имеет простоту развертывания.

Общая архитектура системы ИАС «ЗОО-защита» состоит из подключенных камер и коммутаторов видеонаблюдения (например, входящих в состав АПК «Безопасный город»), сервера хранения данных, анализатора видеопотока, сервера распознавания, модуля уведомления, системы звукового оповещения.

Таким образом, назначение ИАС «ЗОО-защита» состоит в следующем:

- вести учет безнадзорных животных;
- определять места проживания безнадзорных животных;
- помогать в поиске потерявшихся домашних животных;
- определять наличие особей и стай на конкретной территории, их местоположение и перемещение в режиме on-line;
- предупреждать о появлении безнадзорных животных на территории школ, детских садов, социальных объектах, а также на территории промышленных предприятий и коттеджных поселков;
- следить за соблюдением правил выгула домашних животных.

ИАС «ЗОО-защита» позволит:

- предупреждать нападения безнадзорных животных;
- автоматизировано контролировать популяции безнадзорных животных;
- систематизировать имеющиеся данные, формировать отчетность любого типа;
- вести автоматизированный контроль выгула домашних животных в части выполнения требований Федерального закона № 498-ФЗ от 27 декабря 2018 г. (возможно сопряжение с системами автоматического выписывания штрафов за нарушение правил);
- предупреждать граждан о появлении на территории населенных пунктов хищных животных (для крайнего Севера).

Список литературы

1. Об эпизоотологической и эпидемиологической ситуации по бешенству в I полугодии 2022 года в Республике Башкортостан / новость от 20.07.2022 // Официальный сайт Управления Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Республике Башкортостан. URL: https://02.rospotrebnadzor.ru/content/172/41328/?sphrase_id=112371 (дата обращения: 26.07.2022).
2. Образцова Е. С. Разработка универсального мобильного приложения для мониторинга и помощи животным «Второй Дом» // Молодой ученый. 2020. № 22 (312). С. 4–8.
3. Федеральный закон от 27.12.2018 № 498-ФЗ «Об ответственном обращении с животными и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_314646/ (дата обращения: 26.07.2022).

Г. Ф. Якубова,

студент,

Российский государственный университет нефти и газа
имени И. М. Губкина

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ БЛОКЧЕЙН В НЕФТЕГАЗОВОЙ ПРОМЫШЛЕННОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Технология блокчейн в настоящее время часто используется в разных отраслях экономики: это финансы, логистика, страхование, документооборот. Также все больше внимания использованию технологий блокчейна уделяет энергетический сектор. Пользователи блокчейна видят потенциал в упрощении процессов, что приводит к снижению затрат и повышению эффективности. Целью данного исследования выступает выявление приемов и перспектива правомерного использования технологий блокчейна в нефтегазовой промышленности. В условиях ограничительных политических и экономических мер, введенных государствами и международными организациями в отношении Российской Федерации, перед нефтегазовыми компаниями стоят важные проблемы, начиная от крупных капиталовложений в IT-технологии до участившихся кибератак на корпоративные системы, которые требуют новых качественных решений.

Ключевые слова: право, цифровые технологии, блокчейн, безопасность, нефтегазовая промышленность, санкции, эффективность, децентрализация

APPLICATION OF BLOCKCHAIN TECHNOLOGIES IN THE OIL AND GAS INDUSTRY OF THE RUSSIAN FEDERATION

Abstract. Blockchain technology is currently often used in various sectors of the economy – finance, logistics, insurance, document management. Also, the energy sector is paying more and more attention towards the use of blockchain technologies. Blockchain users see the potential in simplifying processes, which leads to lower costs and increased efficiency. The purpose of this study is to identify techniques and prospects for the legitimate use of blockchain technologies in the oil and gas industry. In the context of restrictive political and economic measures imposed by states and international organizations against the Russian Federation, oil and gas companies face important problems, ranging from large investments in IT technologies to frequent cyber-attacks on corporate systems that require high-quality and new solutions.

Keywords: Law, Digital technologies, Blockchain, Security, Oil and gas industry, Sanctions, Efficiency, Decentralization

В настоящее время технология блокчейн является одной из широко обсуждаемых цифровых технологий. Следует отметить, что системы, построенные по принципу блокчейн, представляют цепочку цифровых блоков, каждый из которых безопасен и хранится на различных компьютерах в виде разнесенной системы данных. Единый код, объединяющий все ячейки, подразумевает, что управление информацией и ее анализ осуществляются всеми участниками единой цепочки блоков, объ-

единенных одной общей программой. Данное нововведение, в сравнении с классическими системами хранения данных, позволяет не хранить данные об операциях с блоками на одном компьютере, а задействовать все компьютеры участников сети, что и породило название «блокчейн» (blockchain – «цепочка блоков»). При этом уничтожение нескольких компьютеров не приведет к потере блоков, поскольку информация дублируется на остальных компьютерах. Так как одного места хранения данных нет, то и проверить систему крайне сложно, без ведома хозяина программы третьи лица, в том числе различные преступные группировки, не смогут получить доступ к системе, даже если взломают отдельный компьютер.

В качестве точки, связывающей различные компьютеры, может выступать децентрализованный сервер, которые осуществляет пиринговое соединение с остальными, являясь центром блокчейн-операций. При этом уничтожение сервера не приведет к потере данных блокчейн, достаточно будет подключить новый сервер, и данные с остальных компьютеров, именуемых узлами, или нодами, снова начнут обрабатывать децентрализованный реестр операций. Таким образом, создается база единых данных, которые имеют структуру компьютерного роя, управляемого из многих источников, с высокостащенной системой шифрования. Отсутствие единого центра исключает контроль не только хакерами, но и государственными органами, что является причиной критики технологий блокчейн законодателем.

Технологии блокчейн создают уникальный код, который позволяет при дешифровке получить результат, имеющийся только у обладателя дешифровального ключа. Значит, безопасен и закрыт от мошенников и госслужб. Также немаловажной составляющей изучаемой технологии являются криптографические алгоритмы. В блокчейне операции с активами собираются в отдельные блоки. Данные в каждом блоке кодируются благодаря криптографическим алгоритмам, и каждый этот блок имеет хэш – закодированную запись о предыдущем блоке [1]. Информацию в данном блоке нельзя поменять или стереть, потому что остальные блоки немедленно восполнят изменение за счет хэша, имеющегося в каждом из них. Для полного же доступа к каждому блоку злоумышленнику потребуется знать все ключи, открывающие зашифрованные данные каждого из блоков. Доступный только автору закрытый ключ обеспечивает неизменность данных участниками без соответствующего пересчета контрольной суммы, а открытый ключ, который доступен всем участникам, предоставляет возможность каждому из них верифицировать составляющие блока [2. С. 4–9].

Как пример можно привести токены и криптовалюты, которые являются инструментами инвестирования при минимальном контроле со стороны государства. В настоящее время не существует рычагов правового регулирования в сфере криптовалют и вообще практик регулирования блокчейна. Использование технологии блокчейна для решения различных кейсов (криптовалюта, распределенное хранение и обмен информацией, исполнение контрактов) требует применения правовых норм из различных отраслей. Столкнувшись с этим, законодатель не может выбрать между последовательным расширением традиционных норм и принятием централизованного регулирования для любой децентрализованной системы [3. С. 10].

В мире существует опыт использования блокчейн-технологий для привлечения средств. В том числе в нефтегазовую область. Нефтегазовая отрасль основны-

вается на работе нескольких партнерских предприятий, большинство из которых являются совместными проектами с капиталом различных участников. В свою очередь, деятельность каждого из предприятий подразумевает логистические, финансовые, производственные и иные цепочки от добычи сырья и до конечного потребителя.

Характер деятельности предприятий нефтегазового комплекса подразумевает повышенные требования к системам хранения данных, что могут обеспечить технологии разнесенного хранения зашифрованных данных, в виде блокчейна. Процессы ведения предпринимательской деятельности, бизнеса в нефте- и газодобыче предполагают защиту как от нежелательного внимания третьих лиц, так и защиту от случайной гибели данных. Оба требования достигаются использованием блокчейн-технологий в бизнес-процессах. Создание серверов, объединенных общими программами, работающими по принципу блокчейн, позволяет говорить о повышении качества управления сектором.

В 2017 г. глава Венесуэлы Николас Мадуро объявил о создании в республике собственной криптовалюты El Petro, которая должна помочь стране «продвинуться в вопросе денежного суверенитета» и преодолеть финансовую блокаду. Мадуро сообщил, что Венесуэла принимает El Petro и как суверенный боливар, и как нефтяную валюту. Нефтяная валюта выступает под статусом легальной валюты. Данная валюта будет применяться в ипостаси международной расчетной единицы республики для международных транзакций и также выступать как нефтесервисная валюта для внутренних экономических реформ страны и может использоваться в качестве легального платежного средства для осуществления внутренних налоговых платежей Венесуэлы. Петрокоины, оилкоины – опыт Венесуэлы показывает, что применение технологий возможно, в том числе под государственным контролем [4].

В условиях политического и экономического давления на Россию вопросы обхода санкций приобретают особую актуальность, особенно в нефтегазовой промышленности. Для Российской Федерации, обладающей большими запасами полезных ископаемых ресурсов, имеет смысл оценить ситуацию и перспективы для майнинга. Наша страна имеет все возможности стать лидером в данной отрасли и решить ряд назревших проблем. Почему бы в ограниченном объеме не создать «газпромкоины» или аналогичные блокчейн-токены? В России эти инструменты будут под контролем государства, а для Запада будет крайне сложно вводить санкции, поскольку блокчейн-системы не расшифровываются.

Как пример, можно привести опыт «Газпрома», который дал возможность зарабатывать на криптовалюте обеспеченной нефтью и газом! В меморандуме о сотрудничестве, который подписывался на Петербургском международном экономическом форуме с оператором центров обработки данных BitRiver, упоминается, что бизнес-модель «Газпром нефти» не включает работу с цифровыми валютами – целью компании является развитие новых способов полезного использованияпутного нефтяного газа. Данную модель также возможно использовать для обхода санкций и запустить «газпромкоины» под управлением государства. Такое решение поспособствует укреплению позиции государства на мировом рынке и перешагиванию через все «можно» и «нельзя» [5].

Список литературы

1. Блокчейн – новые возможности для производителей и потребителей электроэнергии? URL: <https://www.pwc.ru/publications/blockchain.html> (дата обращения: 06.09.2022).
2. «Газпром нефть» и BitRiver договорились о развитии энергоемких центров обработки данных. URL: https://www.gazprom-neft.ru/presscenter/news/gazprom_neft_i_bitriver_dogovorilis_o_razvitii_energoemkikh_tsentrov_obrabotki_dannykh (дата обращения: 10.09.2022).
3. Егорова М. А., Белых В. С., Решетникова С. Б. Технология блокчейн: перспективы применения и значение для целей развития информационного общества // Юрист. 2019. № 7.
4. Появилась первая национальная официальная цифровая валюта, а петрокойн Венесуэлы получил «статус фиатной валюты». URL: <https://russianblogs.com/article/36781671800/> (дата обращения: 10.09.2022).
5. Янковский Р. М. Государство и криптовалюты: проблемы регулирования. Московский государственный университет, 2017. URL: <http://msu.edu.ru/papers/yankovskiy/blockchain.pdf> (дата обращения: 05.09.2022).

МУЛЬТИДИСЦИПЛИНАРНЫЙ ХАКАТОН | MULTI-DISCIPLINARY HACKATHON

К. В. Головачев,

студент,

Смоленский филиал

Саратовской государственной юридической академии

О. Н. Куликова,

кандидат юридических наук, доцент,

доцент кафедры уголовно-правовых дисциплин,

Смоленский филиал

Саратовской государственной юридической академии

ЭФФЕКТИВНОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЫ В АНТИКОРРУПЦИОННОЙ ДЕЯТЕЛЬНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Противодействие коррупции актуальными в настоящее время средствами прокурорского реагирования входит в информационно-аналитическое обеспечение, включая программное. Современные коммуникативные (информационно-коммуникационные) средства фиксации, необходимые для деятельности органов прокуратуры, относятся к правовым средствам профилактической направленности по противодействию в сфере коррупции, которые выступают основной целью исследования. Использование в профессиональной деятельности современных информационных систем требует их защищенности, обеспеченности государственными возможностями в силу повышенной прикладной направленности в области коррупционных проявлений. Практический аспект работы связан с определением центральной роли органов прокуратуры Российской Федерации в системе государственных органов по противодействию коррупции. Теоретическое значение исследования отражает системный анализ роли информационной системы Генеральной прокуратуры России по вопросам межведомственного электронного взаимодействия в антикоррупционном направлении.

Ключевые слова: информационная система, прокуратура, электронное взаимодействие правоохранительных органов, антикоррупционная деятельность, коррупция

THE EFFECTIVENESS OF THE INFORMATION SYSTEM OF INTERDEPARTMENTAL ELECTRONIC INTERACTION OF THE PROSECUTOR GENERAL'S OFFICE IN THE ANTI-CORRUPTION ACTIVITIES OF THE RUSSIAN FEDERATION

Abstract. Combating corruption by currently relevant means of prosecutorial response is included in the information and analytical support, including software.

Modern communicative (information and communication) means of fixation, necessary for the activities of the prosecutor's office, belong to the legal means of preventive focus on combating corruption, which are the main purpose of the study. The use of modern information systems in professional activity requires their security, provision with state capabilities due to the increased application orientation in the field of corruption manifestations. The practical aspect of the work is connected with the definition of the central role of the Prosecutor's Office of the Russian Federation in the system of state bodies for combating corruption. The theoretical significance of the study reflects a systematic analysis of the role of the information system of the Prosecutor General's Office of Russia on interdepartmental electronic interaction in the anti-corruption direction.

Keywords: information system, prosecutor's office, electronic interaction of law enforcement agencies, anti-corruption activities, corruption

Введение. Актуальность исследования определяется необходимостью активного использования при осуществлении надзорных мероприятий специализированных информационных ресурсов и информационной системы межведомственного электронного взаимодействия Генеральной прокуратуры Российской Федерации (ИС МЭВ) [1].

Авторское исследование опирается на труды Э. Б. Хатова (2016), Т. М. Кебекова (2012), М. В. Рубцовой (2020), чьи работы посвящены изучению вопросов информационного обеспечения прокурорского надзора за исполнением законов о противодействии коррупции, путей повышения эффективности информационно-аналитической работы в органах прокуратуры. Материал базируется на исследованиях А. П. Брагина и А. Д. Пронякина (2007), О. Н. Куликовой (2022), в которых отражается ключевое место органов прокуратуры в противодействии коррупции и предлагаются государственные меры такого противодействия, включающие информационно-правовой характер.

Деятельность органов российской прокуратуры на современном этапе развития общества свидетельствует о возложении на нее государством такой функции, как противодействие преступности, в том числе коррупционных проявлений, в качестве фундаментального блока профессиональной деятельности. Правоохранительная служба органов прокуратуры в данном направлении отражает актуальность формирования политики государства на федеральном и муниципальном уровне в связи с сущностью негативного социального явления – коррупции.

Коррупция, это социальное зло, которое присутствовало всегда, и признавалось государством как неизбежная общественная и государственная издержка. Общественные отношения не стояли на месте и развивались, и коррупция развивалась вместе с ними. Такое явление влияет не только на доверие граждан государству, но и напрямую затрагивает экономическую безопасность государства. С каждым годом формы проявления коррупции изменялись, и в силу таких изменений государство все чаще приходило к выводу о необходимости ужесточения борьбы с ней.

Механизм противодействия коррупции в России – это комплекс мероприятий социально-правового, организационного, управленческого и нравственно-этиче-

ского характера, обеспечиваемый государственными органами в целях предотвращения коррупционных проявлений со стороны работников государственных органов и их должностных лиц [2]. Данный механизм противодействия коррупционных деяний должен охватывать, по нашему мнению, такие меры со стороны политики государства как организационно-управленческие, воспитательно – правовые меры в сфере деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, институтов гражданского общества, социально – правовые меры в контексте действующего законодательства Российской Федерации. Тем самым, следует, что информационную систему Генеральной прокуратуры следует рассматривать как эффективное направление противодействия коррупции организационно-управленческого и правового характера.

Как справедливо отмечает Т. М. Кебеков: «...важно, чтобы работа по сбору информации о состоянии законности носила системный характер. В этих целях прокуроры городов, районов области ежемесячно издаются информационно-аналитические сборники об итогах работы органов прокуратуры и иных правоохранительных органов города, района по укреплению законности и правопорядка, усилению борьбы с преступностью» [3]. В научном материале прокурор Псковской области подчеркнул, что информационно-аналитическая работа является одним из важнейших элементов организационного обеспечения деятельности органов прокуратуры.

Развитие технологий сильно повлияло не только на формы проявления коррупции, но и на методы борьбы с ней. Особое положение органов прокуратуры обусловлено местом прокуратуры в системе органов государственной власти. Прокуратура не относится ни к одной из ветвей власти, а в борьбе с коррупцией выступает координирующим и надзорным органом. Информационно-аналитическая деятельность органов прокуратуры включает информационное и аналитическое обеспечение. Некоторые авторы полагают, выделяя информационную составляющую, что подобное обеспечение деятельности прокуратуры – это процесс подбора, обработки информационных материалов, предназначенных для анализа, планирования и контроля [4].

По мнению А. Б. Хатова, с чьим мнением мы согласны, речь в случае информационного обеспечения может идти только о сборе, учете, накоплении информации, ее обмене, так как ее обработка (кроме технической) предполагает интеллектуальную, т. е. аналитическую, составляющую [5]. Под информацией в системе прокуратуры автор понимает сведения (сообщения, данные), принятые, понятые, оцененные как полезные для осуществления прокурорской деятельности независимо от формы их представления [6]. Информационное обеспечение в прокурорской деятельности имеет цель соблюдения укрепления законности, единства и верховенства закона, оно включает получение информации, анализ ее источников, сбор, накопление, ведение учета.

Результаты исследования. Надзор за соблюдением антикоррупционного законодательства является одним из приоритетных видов надзорной прокурорской деятельности. К настоящему времени разработаны и применяются порядка две-

надцати информационных систем и комплексов, которые использует прокуратура в своей повседневной работе. Так, в рамках осуществления надзора, прокуроры проверяют соблюдение государственным служащим требований Федерального закона от 03.12.2012 года № 230-ФЗ «О контроле за соответствием расходов лиц, замещающих государственные должности и иные лица». В рамках данного надзора сотрудники прокуратуры проверяют и анализируют соответствие справок о доходах как самих должностных лиц, так и членов их семей. Своевременное создание в 2019 г. нормативных и организационных предпосылок для повышения эффективности надзорной деятельности в части соблюдения запрета отдельным категориям лиц открывать и иметь счета (вклады), хранить наличные денежные средства и ценности в иностранных банках, расположенных за пределами территории Российской Федерации, владеть и (или) пользоваться иностранными финансовыми инструментами может стимулировать выявление органами прокуратуры нарушений имеющегося антикоррупционного запрета [7] (в 2019 г. – 8, в 2018 г. – 15 [8]).

Тем самым технологическое развитие принесло довольно важные изменения в данный процесс. Так, в осуществление такого надзора в помощь сотрудникам прокуратуры приходила информационная система межведомственного электронного взаимодействия генеральной прокуратуры РФ (далее ИС МЭВ ГП РФ). Она помогает взаимодействовать органам прокуратуры. Самыми востребованными данными, запрашиваемыми в ИС МЭВ ГП РФ, является информация об учредителях, о доходах физических лиц. В этой программе сотрудники прокуратуры могут оперативно получать необходимую им информацию, в частности, из таких как МВД России, ФНС России, Росреестр.

В рамках работы с ИС МЭВ ГП РФ сотрудники прокуратуры могут сами выбирать необходимую им информацию и ведомство. Механизм осуществления запроса довольно прост, нужно ввести необходимые данные, которые варьируются от ведомства к ведомству. По общему правилу для осуществления запроса им нужно знать ФИО лица, дату его рождения, в отдельных случаях СНИЛС или ИНН. Благодаря возможности отправлять большое количество запросов в одной информационной системе сотрудники более продуктивно собирают необходимую им информацию от различных ведомств, при этом уменьшая количество бумажного документооборота. Это позволяет более эффективно осуществлять надзор за соблюдением антикоррупционного законодательства, и оперативно получать необходимую информацию для осуществления данного вида надзора. Само по себе электронное взаимодействие органов прокуратуры с различными ведомствами способствует уменьшению коррупциогенных фактор при их межведомственном взаимодействии.

Обсуждение. Вся фактическая деятельность современных органов прокуратуры Российской Федерации связана с получением, накоплением, обработкой, учетом получаемой информации. Данные о коррупционных проявлениях в государственных, муниципальных, частных и иных поведенческих актах находят отражение в системе информационного пространства прокурорской деятельности. Информация аккумулируется из многообразных источников, характеризуется

постоянно нарастающим объемом, удельным весом процедур изучения и обработки, многократным повторением циклов получения информации, ее отправки. Результатом такой деятельности выступает подготовка и принятие решений с позиций конфиденциальности, структурированности и важности. Информация должна обеспечиваться полнотой и достоверностью, что свидетельствует об истинных данных, внесенных в информационную систему межведомственного электронного взаимодействия Генеральной прокуратуры России в вопросах антикоррупционного направления. Качество информации состоит в степени расширения полезной совокупности сведений и смысловых связей между ними. Адекватность информации характеризуется уровнем соответствия информационного образа реальному состоянию объекта. Как отмечают информационные источники: «Нередко информация, которой располагает прокурор, противоречива и недостаточна, что существенно осложняет работу» [9].

В настоящее время в современной России единая система сбора и обработки получаемой информации как важное направление государственного учета документов отсутствует. Соответственно должным образом не функционирует сбор, регистрация, обработка, хранение информации, которая характеризовала бы с исчерпывающей полнотой то или иное направление прокурорской деятельности.

Ранее проведенные исследования в области современных информационных технологий правоохранительных органов, включая органы прокуратуры, и российских информационно-консультационных систем, включающих данные о коррупционных проявлениях, не охватывали информационную систему межведомственного электронного взаимодействия Генеральной прокуратуры России по вопросам антикоррупционной деятельности. Наше исследование позволяет определить ее эффективность, что, в свою очередь, актуально обусловит необходимость соответствующей государственной защиты и поддержки, программно-технического обеспечения и оснащения.

Заключение. Удобство и оперативность при использовании ИС МЭВ ГП РФ помогает сотрудникам своевременно реагировать на нарушение антикоррупционного законодательства должностными лицами. В последнее время количество запросов, направленных на проведения проверки за соблюдением антикоррупционного законодательства, значительно увеличивается. Благодаря этой системе органами прокуратуры было пресечено достаточное количество нарушений антикоррупционного законодательства, и виновные привлекались к ответственности в соответствии с действующим законодательством. На данный момент совершенствуется и расширяется данная информационная система. Данная работа невозможна без совместного и плодотворного труда заинтересованных ведомств. На сегодняшний день в рамках развития ИС МЭВ ГП РФ осуществляется большое количество модернизационных мер, направленных на улучшение работы и повышение отказоустойчивости данной системы.

Исходя из вышеизложенного, можно сделать вывод, что общество не стоит на месте и постепенно развивается, но совместно с развитием общества развиваются и его главные пороки, в частности развивается и коррупция, приобретая все новые и новые формы. Но совместно с совершенствованием форм коррупционных

проявлений необходимо развитие и механизмов противодействия ем. ИС МЭВ ГП РФ – это один из новых механизмов взаимодействия заинтересованных органов, направленный на изобличение, предотвращение и привлечения к ответственности лиц, нарушивших антикоррупционное законодательство. На данный момент времени данная система зарекомендовала себя как эффективный и действенный способ противодействия коррупционному поведению. Не смотря на то, что данная система хорошо себя зарекомендовала, она продолжает развиваться и модернизироваться для улучшений дальнейшего взаимодействия правоохранительных органов, в частности в вопросах противодействия коррупции.

Противодействие коррупции средствами прокурорского надзора представляет собой информационно-аналитическую деятельность, основу которой составляет программное информационное обеспечение в виде информационной системы межведомственного электронного взаимодействия Генеральной прокуратуры Российской Федерации, направленной на обеспечение и выполнение антикоррупционной деятельности. Такая система требует государственной охраны и соответствующего материально-технического и информационно-ресурсного обеспечения.

Список литературы

1. Генеральная прокуратура: [сайт]. URL: https://epp.genproc.gov.ru/web/gprf/expert_advice/news?item=62098037
2. Куликова О. Н. Современная юриспруденция: теория, методология, практика: материалы Международной научно-практической конференции 30 ноября 2021 г. (Липецк) / под общ. ред. д.и.н., проф. В. В. Соловьевой. Воронеж, 2022. С. 75–79.
3. Кебеков Т. М. Пути повышения эффективности информационно-аналитической работы в органах прокуратуры // Вестник Академии Генеральной прокуратуры Российской Федерации. 2012. № 6. С. 13–16.
4. Брагин А. П., Пронякин А. Д. Прокурорский надзор в Российской Федерации. М.: Изд. центр ЕАОИ, 2007. 204 с.
5. Хатов Э. Б. Вопросы информационного обеспечения прокурорского надзора за исполнением законов о противодействии коррупции // Журнал зарубежного законодательства и сравнительного правоведения № 4. 2016. С. 34-40.
6. Хатов Э. Б. Информационное обеспечение деятельности прокуратуры // «Черные дыры» в российском законодательстве. 2007. № 4. С. 385–388.
7. Рубцова М. В. Деятельность органов прокуратуры Российской Федерации в сфере противодействия коррупции // The scientific heritage. No 57 (2020). С. 17–21.
8. Состояние законности и правопорядка в Российской Федерации и работа органов прокуратуры. 2019 год: информ.-аналит. записка / под общ. ред. ректора Университета прокуратуры Российской Федерации д-ра юрид. наук, проф. О. С. Капинус. М.: Ун-т прокуратуры Рос. Федерации, 2020. 232 с.
9. Информатизация органов прокуратуры Российской Федерации. URL: https://studme.org/70156/pravo/informatizatsiya_organov_prokuratury_rossiyskoy_federatsii

Ю. В. Ершова,

кандидат юридических наук,
доцент кафедры гражданского права и процесса,
Оренбургский институт (филиал)
Университета имени О.Е. Кутафина

В. К. Лысенко,

студент,
Оренбургский институт (филиал)
Университета имени О.Е. Кутафина

КРИПТОВАЛЮТА КАК ОБЪЕКТ КОРПОРАТИВНОГО ПРАВА: ТЕНДЕНЦИИ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА

Аннотация: В статье анализируется гражданско-правовое регулирование криптовалюты и возможности реализации данного регулирования в корпоративных отношениях, применения ее при использовании в качестве имущества корпорации либо при создании корпорации. Изучены позиции ученых о правовой природе криптовалюты, ее видах и формах воплощения. Рассмотрены тенденции дальнейшего развития данной категории объектов права в российском законодательстве, а также варианты использования криптовалюты в современных корпоративных отношениях.

Ключевые слова: цифровые технологии, криптовалюта, виртуальная валюта, объекты корпоративных прав, цифровые права, биткоин, цифровые финансовые активы.

CRYPTOCURRENCY AS AN OBJECT OF CORPORATE LAW: TRENDS IN THE DEVELOPMENT OF LEGISLATION

Abstract. The article analyzes the civil law regulation of cryptocurrency and the possibility of implementing this regulation in corporate relations, its application when used as property of a corporation or when creating a corporation. The positions of scientists on the legal nature of cryptocurrency, its types and forms of implementation are studied. The trends of further development of this category of objects of law in Russian legislation, as well as options for using cryptocurrency in modern corporate relations are considered.

Keywords: digital technologies, cryptocurrency, virtual currency, objects of corporate rights, digital rights, bitcoin, the latest objects of law, digital financial assets

Цифровизация процессов во всех общественных отношениях в современности является абсолютным трендом развития. Теория права и законодательство не могут отставать от данного развития. Это дает почву для формирования множества идей, взглядов, и, как следствие, научных трудов. Таковыми являются как серьезные комплексные издания на уровне учебников [9. С. 7–15], так и публикации, затрагивающие отдельные аспекты соответствующих технологий [1. С. 163–166].

В силу развития технологического прогресса, процессов глобализации и интеграции, развитие цифровых прав получило широкое развитие во всем мире, и Россия не является исключением. Под влиянием данных событий получила развитие так называемая криптовалюта, ее широкое распространение было обусловлено частыми экономическими кризисами и нарастающим недовольством всемирной банковской системой, ее централизованным контролем, и криптовалюта в данном разрезе выступает как альтернативное средство накопления и платежа, в том числе и в корпоративных отношениях. Уже встречаются случаи оплаты криптовалютой вносимого вклада в уставный капитал, оплата долгов в предбанкротных отношениях. Это влечет необходимость понимания сущности данного объекта корпоративных прав.

Как известно, существует две разновидности виртуальных валют – открытая и закрытая. Открытая валюта обладает эквивалентной стоимостью, выраженной в реальной национальной валюте, наиболее популярная криптовалюта – биткоин появилась в 2009 году, в 2011 году приобрела популярность. Сатоши Накамото предполагал использование биткоина как средства платежа для упрощения денежных переводов. Закрытая валюта предназначается для использования, например, в многопользовательских онлайн-играх. Иначе говоря, использование закрытой валюты довольно ограничено ввиду ее специфической цели. В корпорациях использование ее на современном этапе невозможно.

Централизованные открытые виртуальные валюты подконтрольны администратору, а децентрализованные открытые как раз и являются «криптовалютами». К ним относится и самая распространенная – биткоин [5. С. 1–9]. Децентрализованность и открытость обеспечили стремительное развитие целого ряда иных криптовалют – «Эфириум», «Рипл», «Лайткоин» и т.д.

Исходя из российского и зарубежного права термин «криптовалюта» (в российском законодательстве закреплена дефиниция «цифровые активы», этот термин отличается от термина «криптовалюта») в настоящее время не выделен.

Так, например, Д. С. Вахрушев и О. В. Железов дают собственное определение криптовалюте, говоря о разновидности электронных денег, представляющих собой сложную систему информационно-технологических процедур, построенных на криптографической защите, регламентирующих идентификацию владельцев и фиксацию их смены, функционирование которых основано на децентрализованном механизме эмиссии и обращении [3. С. 2–3].

Криптовалюта – разновидность цифровой валюты, учет внутренних расчетных единиц которой обеспечивает децентрализованная платежная система без администратора или его аналога. Также термин «криптовалюта» раскрывает наиболее популярная криптовалютная биржа Binance – это особая форма электронных денег, которые хранятся не на централизованном счете, а в сети блокчейн [4].

Здесь же раскрывается суть технологии блокчейна: «Блокчейном называют виртуальную базу данных, где фиксируется информация обо всех транзакциях и о том, сколько монет хранится на счете. Эта технология обеспечивает возможность переводить активы между пользователями, выступая бесспорной гарантией владения активами».

Выше мы указывали, что в законодательстве термин «криптовалюта» не закреплен, однако дефиниция «биткоин» закреплена. Это стало возможным благодаря принятию Закона о легализации биткоина как платежного средства в Сальвадоре [7].

Под биткоином понимается «тип криптовалюты использующей технологию Blockchain, и законное платежное средство в Сальвадоре согласно закону Bitcoin. Как мы видим данная дефиниция мало раскрывает содержание и суть данного объекта [14].

По мнению ученых, криптовалюте присущи три признака – анонимность, децентрализованность и трансграничность [6. С. 84].

Как отмечает Л. Б. Нигматулина, все государства мира можно разделить на три большие группы:

1. Осуществляющие регулирование криптовалюты (Япония, США, Великобритания и т. д.).
2. Регулирование отсутствует или находится в стадии становления (Российская Федерация).
3. Криптовалюта запрещена (Китай, Боливия, др.).

Формы регулирования криптовалют в национальных правовых системах могут быть совершенно разными: от запрета (Боливия, Китай) через ограниченное признание (Дания) до признания в качестве полноценной валюты (Швеция) [9. С. 18]. Как было указано выше Сальвадор является единственной страной, где криптовалюта (биткоин) признана в качестве законного средства платежа.

Россия имеет большие перспективы в развитии рассматриваемого блока актов. Стоит отметить, что уже имеющийся накопленный опыт регулирования оборота цифровых активов в других государствах может быть критически оценен, подвергнут анализу и грамотно заимствован, трансформирован под запросы и формат российского законодательства.

Проведем анализ существующих норм для выяснения правового режима криптовалюты.

1 октября 2019 г. вступил в силу ФЗ от 18.03.2019 № 34-ФЗ «О внесении изменений в части I, II и статью 1124 части III ГК РФ», согласно которому статья 128 части первой ГК РФ дополнена указанием на цифровые права.

Законом о цифровых правах эти права отнесены к числу имущественных наряду с безналичными денежными средствами и бездокументарными ценными бумагами (ст. 128 ГК РФ).

Особое внимание здесь стоит уделить дефиниции «цифровых прав», которая стала новой и является базисной для понимания места криптовалюты в гражданском законодательстве. В п. 1 новой ст. 141.1 ГК РФ закреплена дефиниция цифровых прав. Можно сказать, что «цифровые права» - это обозначение зафиксированных в электронной форме имущественных прав, отвечающих двум признакам: они должны быть прямо названы в качестве цифровых в законе; сделки с ними должны проводиться на информационной платформе, «отвечающей установленным законом признакам» [8. С. 11–12].

ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ» от 31.07.2020 № 259-ФЗ, который вступил в силу 01 января 2021 года, направлен на введение базы для обращения цифровых финансовых активов и цифровой валюты в России.

В законе вместо термина «криптовалюта» используется термин «цифровая валюта». Основные признаки ее заключены в следующем:

- это совокупность электронных данных (код или обозначение) в системе;
- валюта трактуется как инвестиции или средство платежа, которое не является денежной единицей;
- в отношении цифровой валюты по общему правилу нет лица, обязанного перед каждым обладателем таких электронных данных [7].

Цифровые финансовые активы представляют собой подмножество цифровых прав, которые включают в себя: денежные требования, возможность осуществлять права по эмиссионным ценным бумагам, доля в капитале акционерного общества, а также право требовать передачи эмиссионных ценных бумаг [2. С. 3].

Правовому регулированию криптовалюты был дан новый импульс концепцией Минфина по законодательному регламентированию механизмов организации оборота цифровых валют, которая была утверждена Правительством РФ. Рассмотрим данную концепцию наиболее подробно, так как многие ее положения могут лечь в основу будущего законопроекта.

В своей концепции Минфин предлагает проводить все операции с криптовалютами через банки РФ, устанавливать личность держателей криптокошельков и делить их на квалифицированных и неквалифицированных инвесторов. По оценкам экспертов, на которые ссылается министерство, гражданами России открыто несколько миллионов криптовалютных кошельков, объем средств на которых составляет около 2 трлн рублей.

Проведение операций через банки, как считает Министерство финансов, позволит обеспечить надлежащий контроль за такими операциями и идентификацию всех участников.

Документ концентрируется исключительно на наиболее непрозрачном, но наиболее выгодном для государства сегменте – сделках с криптовалютой. Реализация концепции, позволит обложить всех его участников налогом.

Концепция подразумевает внедрение исключительно удобной для полного контроля транзакций государством замкнутой системы «банк – биржа – клиент». Именно банки будут являться «организаторами системы обмена цифровых валют».

Вводится понятие «оператора обмена цифровых валют», которые признаются организациями, осуществляющим операции с денежными средствами. Они разделены на два вида: обладающих базовыми и универсальными правами. Все лица будут обязаны открывать электронные кошельки в банках-операторах, быть включенными в соответствующий Реестр, который, предполагаемо, будет вести ЦБ РФ. Также говорится о необходимости определенного уставного капитала, точный размер концепция не разъясняет.

В концепции обсуждается и регулирование деятельности иностранных бирж. Главный посыл заключается в том, что иностранным биржам необходимо будет

открывать свои представительства на территории РФ и включаться в систему экосистему по операциям с криптовалютой.

Клиентами по сделкам с криптовалютой теперь могут являться как физические, так и юридические лица. Эволюция просматривается во включении в субъектный состав юридических лиц, это усиливает потенциал рассматриваемых отношений.

Даже поверхностный анализ Концепции показывает, что действия Министерства финансов направлены на легализацию и вывод «из тени» операций по купле-продаже цифровой валюты. Более того, видится серьезная доходность бюджета с учетом выявленного оборота средств (см. выше).

Однако собственно правовой режим криптовалюты концепция ясно не определяет. Минфин опирается на положения Закона о цифровых активах в определении сущности криптовалюты. При этом отождествляются дефиниции цифровой валюты и криптовалюты, ранее этого не было отражено в федеральном законодательстве.

На момент написания данной статьи ведется дискуссия на тему регулирования криптовалют между Минфином РФ и ЦБ РФ. Позиция Минфина более либеральна и открыта, позиция же ЦБ РФ прямо противоположная, настаивается на ограничении инвестиций в криптовалюту, ограничении субъектов цифрового оборота и введении административного и уголовного преследования. Президент РФ В. В. Путин призвал ЦБ РФ и Минфин прийти к скорейшему решению спора [8].

Таким образом, российское законодательство движется в сторону восполнения пробелов, связанных с правовым режимом криптовалюты. Действия законодателя следует рассматривать позитивно, идет работа по внедрению в правовое поле РФ нового объекта гражданского, следовательно, и корпоративного, права. Здесь же стоит отметить, что многие аспекты еще не освещены и не проработаны, особое внимание стоит уделить механизму учета данных (реестр данных) объектов гражданских прав, а также выработать механизм и гарантии восстановления нарушенных прав и законных интересов. Следует помнить, что регулирование криптовалюты неразрывно связано с институтом гражданско-правовой ответственности ввиду сложности доказывания нарушений в рассмотренной сфере.

Криптовалюта получит дальнейшее развитие в нашей стране, что позволит России быть конкурентоспособной в развитии цифровых платежных технологий и привлекать инвестиции в бизнес в большем масштабе.

Список литературы

1. Белова Н. Ю. Концепция правового регулирования оборота криптовалюты в Российской Федерации // Высокие технологии, наука и образование: актуальные вопросы, достижения и инновации: сборник статей XIV Всероссийской научно-практической конференции, Пенза, 23 января 2022 г. 2022. С. 163–166.

2. Васильева В. С. Правовой режим цифровых финансовых активов на основе анализа ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ» // StudNet. 2021. № 6. С. 1–8.

3. Вахрушев Д. С., Железов О. В. Криптовалюта как феномен современной информационной экономики: проблемы теоретического осмысления // Наукоеведение. 2014. № 5. С. 1–9.

4. Виды криптовалют – какие существуют и чем отличаются // Binance URL: <https://www.binance.com/ru/blog/all/виды-криптовалют--какие-существуют-и-чем-отличаются-421499824684902939> (дата обращения: 17.08.2022).

5. Гаврилов В. Н., Рафиков Р. М. Криптовалюта как объект гражданских прав в законодательстве России и ряда зарубежных государств // ВЭПС. 2019. № 1. С. 51–59.

6. Егорова М. А., Кожевина О. В. Место криптовалюты в системе объектов гражданских прав // Актуальные проблемы российского права. 2020. № 1 (110). С. 81–92.

7. Путин вмешался в спор ЦБ и правительства о запрете криптовалют // РБК URL: <https://www.rbc.ru/finances/26/01/2022/61f15f059a79471abff191e> (дата обращения: 17.08.2022).

8. Рожкова М. А. Цифровые права: публично-правовая концепция и понятие в российском гражданском праве // Хозяйство и право. 2020. № 10. С. 3–12.

9. Цифровое право / А. Дюфло, Л. В. Андреева, В. В. Блажеев [и др.]. М.: Издательство Проспект, 2020. 640 с.

М. Ю. Карпухин,

кандидат сельскохозяйственных наук,
проректор по научной работе и инновациям,
Уральский государственный аграрный университет

М. А. Хомякова,

магистр садоводства,
специалист по выставочной и грантовой деятельности,
Уральский государственный аграрный университет

ПЕРСПЕКТИВЫ ЦИФРОВИЗАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА ДО 2030 ГОДА: ПРАВОВОЙ АСПЕКТ

Аннотация. В статье рассматривается возможность цифровизации сельского хозяйства в России в период с настоящего времени до 2030 года с точки зрения правовых актов и возможности реализации обозначенных в них реализации целей. Отмечена важная роль сельского хозяйства как сектора российской экономики и лидирующая роль российского сельского хозяйства на мировом рынке. Анализ экспертных мнений показал, что цифровизация является необходимым условием для дальнейшего успешного развития отечественного сельского хозяйства. Этот вывод обусловлен тем, что отрасли, связанные с сельским хозяйством, цифровизируются, следовательно, чтобы сельское хозяйство продолжало коррелировать с остальными отраслями, включая электроэнергетический сектор, необходима цифровизация агро-промышленного комплекса России. Несмотря не то что Россия занимает лидирующие позиции в мировом сельском хозяйстве, она от-

стает в сельско-хозяйственной цифровизации, что может стать риском ухудшения сельско-хозяйственных показателей в целом. Анализ мнений ученых в области аграрного права показал скептическое отношение к достижению целей в области цифровизации российского сельского хозяйства к 2030 году, поскольку на данный момент цифровизация российского агропромышленного комплекса находится на начальном уровне. Тем не менее авторы статьи приходят к выводу, что развитие цифровизации сельского хозяйства в России вполне возможно, поскольку данная отрасль обладает высоким потенциалом.

Ключевые слова: сельское хозяйство, агропромышленный комплекс, аграрное право, международное право, цифровизация

PROSPECTS OF DIGITALIZATION OF AGRICULTURE UNTIL 2030: LEGAL ASPECT

Abstract. This article examines the possibility of digitalization of agriculture in Russia in the period from now to 2030 from the point of view of legal acts and the possibility of implementing the goals outlined in these acts. The article highlights the important role of agriculture as a sector of the Russian economy and the leading role of Russian agriculture in the world market. The analysis of expert opinions showed that digitalization is a necessary condition for the further successful development of domestic agriculture. This conclusion is due to the fact that agriculture-related industries are digitalizing, therefore, in order for agriculture to continue to correlate with other industries, including the electric power sector, digitalization of the agro-industrial complex of Russia is necessary. Also, this study showed that Russia occupies a leading position in world agriculture, but lags behind in agricultural digitalization, which may become a risk of deterioration of agricultural indicators in general. The study of international regulations and legislation of the Russian Federation allowed us to conclude that the legislator understands the importance of digitalization of the agricultural sector and prioritizes the development of digitalization in agriculture in Russia until 2030. An analysis of the opinions of scientists in the field of agrarian law showed their skeptical attitude towards achieving the goals set by the law in the field of digitalization of Russian agriculture by 2030, since at the moment the digitalization of the Russian agro-industrial complex is at an initial level. The authors of this article, however, conclude that the development of digitalization of agriculture in Russia is quite possible, since this industry has high potential.

Keywords: agriculture, agro-industrial complex, agrarian law, international law; digitalization

Сельское хозяйство на протяжении всей истории занимало важную роль в развитии нашего отечества. Россия всегда позиционировалась на внутреннем и международном рынке как ведущая аграрная держава, обладающая достаточными природными и трудовыми ресурсами, чтобы не только обеспечить свое население должным уровнем продовольствия, но и быть полноценным субъектом международных отношений в сфере мирового агропользования.

Будучи одним из лидеров по показателям в сфере сельского хозяйства в целом, Россия занимает лишь 15-е место по степени цифровизации данной отрасли [1]. Ученые в области аграрного права отмечают, что опыт мирового сельского хозяйства показывает: сегодня наибольшую эффективность в аграрной отрасли гарантирует использование цифровых технологий. Это касается как экономических [2], так и производственных показателей сельскохозяйственной производительности [3], поскольку многие отрасли в настоящее время переходят на цифровую сферу. В условиях глобализации многие сферы жизни находят все больше точек соприкосновения и развитие цифровых технологий в одной части жизни незамедлительно отражается на других: сегодня цифровизация электроэнергетики находит свое отражение во многих сферах жизни [4; 5]. Электричество является незаменимой материей, обеспечивающей жизнедеятельность современного человека, в том числе сельскохозяйственную деятельность. Цифровизация в электроэнергетической сфере уже влияет на агропромышленный комплекс России: например, обеспечение электричеством на фермах уходит в цифровой режим [6; 7]. Сопоставив вышеизложенное, можно сделать вывод, что если не развивать цифровые технологии в отечественном агропромышленном комплексе, Российская Федерация рискует потерять устойчивые позиции и высокие показатели в мировом сельскохозяйственном производстве.

Итак, переход на цифровизацию сельского хозяйства обусловлен не только мировыми тенденциями и нормами международного права, но и цифровизацией связанных с сельским хозяйством отраслей.

Как и всякое явление, цифровизация российского сельского хозяйства регулируется нормами права различных уровней.

Сегодня в Российской Федерации действует ряд нормативных правовых актов, направленных на развитие сельского хозяйства в нашей стране. Согласно тексту ч. 2 ст. 5 Федерального закона от 29.12.2006 № 264-ФЗ «О развитии сельского хозяйства», основными целями государственной аграрной политики являются:

- 1) повышение конкурентоспособности российской сельскохозяйственной продукции и российских сельскохозяйственных товаропроизводителей, обеспечение качества российских продовольственных товаров;
- 2) обеспечение устойчивого развития сельских территорий, занятости сельского населения, повышения уровня его жизни, в том числе оплаты труда работников, занятых в сельском хозяйстве;
- 3) сохранение и воспроизводство используемых для нужд сельскохозяйственного производства природных ресурсов;
- 4) формирование эффективно функционирующего рынка сельскохозяйственной продукции, сырья и продовольствия, обеспечивающего повышение доходности сельскохозяйственных товаропроизводителей и развитие инфраструктуры этого рынка;
- 5) создание благоприятного инвестиционного климата и повышение объема инвестиций в сфере сельского хозяйства;
- 6) наблюдение за индексом цен на сельскохозяйственную продукцию, сырье и индексом цен (тарифов) на промышленную продукцию (услуги), используемую

сельскохозяйственными товаропроизводителями, и поддержание паритета индексов таких цен (тарифов).

Для иллюстрации заинтересованности государства в развитии национального сельского хозяйства была взята именно эта правовая норма, поскольку в названии упомянутого Федерального закона в декларативном порядке зафиксирована основная цель его принятия, а именно развитие сельского хозяйства.

Подзаконные акты также говорят о приоритете развития данной отрасли, причем в ближайшее время. В распоряжении Правительства РФ от 31.12.2020 № 3684-р «Об утверждении Программы фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021–2030 годы)» раздел 4.1 посвящен сельскому, а также близкому ему лесному и рыбному хозяйствам.

В Указе Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» сказано, что к 2024 году формирование ВВП в сельскохозяйственной отрасли должно составлять не менее 20 %.

Российская Федерация является частью международного общества, и, как было сказано ранее, разделяет цели международного развития, в том числе в сельскохозяйственной отрасли. Важным международным документом в системе аграрного российского законодательства является Резолюция Генеральной Ассамблеи ООН, принятая в 2015 году по итогам Саммита «Преобразование нашего мира: повестка дня в области устойчивого развития на период до 2030 года». Согласно п. 59 Повестки 2030, среди значимых задач – удвоение продуктивности сельского хозяйства и доходов мелких производителей продовольствия. 15 марта 2022 года была принята Рекомендация Коллегии Евразийской экономической комиссии от 15.03.2022 № 8 «О стимулировании использования технологий точного земледелия в государствах - членах Евразийского экономического союза», обозначившая среди своих целей применение новых решений, направленных на повышение эффективности, увеличение производительности и обеспечение принципов устойчивого развития сельского хозяйства путем внедрения современных технологических решений в области растениеводства в государствах-членах ЕАЭС.

Изучение национального законодательства, проведенный выше, говорит о том, что, формируя собственную правовую систему, направленную на развитие сельского хозяйства, Россия во многом опирается на акты международного права [8].

Анализ нормативных актов Российской Федерации, проведенный выше на страницах настоящего исследования, показывает, что правящие субъекты нашей страны осознают необходимость внедрения цифровых технологий в сельскохозяйственный сектор, однако эти нормы носят указательный характер, который, по мнению ряда ученых, не отражает существующую действительность [9]. Цифровизация сельского хозяйства на данном этапе развития находится на начальном уровне [10]: недостаток научно-технических знаний, не всегда точные прогнозы развития, а также неразвитость логистических систем приводит к высоким издержкам в сфере цифровизации сельского хозяйства в России [11].

Тем не менее анализ литературы и практики позволяет сделать вывод, что цифровое будущее для российского сельского хозяйства находится не за горами

[12]: несмотря на описанные выше нюансы, российский агро-промышленный комплекс остается одним из сильнейших в мире, поэтому цели усиления цифровизации в сельско-хозяйственной отрасли до 2030 года, как того требуют нормативные акты, могут быть достигнуты, но с гораздо большими усилиями, чем предполагалось изначально.

Следует признать, что цифровизация российского сельского хозяйства необходима в силу ряда причин:

– связанные с сельским хозяйством отрасли переходят на цифровизацию, и, чтобы продолжать взаимодействие с ними, сельскому хозяйству также необходимы аналогичные модернизации;

– цифровизация сельского хозяйства является мировой тенденцией, и чтобы оставаться сильным субъектом на глобальном рынке, России необходимо цифровизировать данную отрасль.

Международные нормативно-правовые акты говорят о необходимости развития цифровизации сельского хозяйства. Россия является частью мирового сообщества, в том числе в правовой сфере: нормы национального права поддерживают мировую тенденцию цифровизации сельского хозяйства. На данном этапе развития аграрного законодательства можно выявить ряд документов, ставящих целью усилить цифровизацию сельского хозяйства в России до 2030 года.

Несмотря на то что ряд ученых ставит под сомнение возможность реализации планов по цифровизации сельского хозяйства в соответствии со сроками, указанными в соответствующих нормативных актах, аргументируя это мнение тем, что на современном этапе цифровизация сельского хозяйства в России находится на начальном уровне и носит весьма скромный характер, достижение цели в виде глобальной цифровизации сельского хозяйства в России может быть достигнуто за счет мощного развития сельскохозяйственной отрасли в нашей стране в целом.

Список литературы

1. Попова О. В. Проблемы правового регулирования цифровизации в агро-промышленном комплексе // Аграрное и земельное право. 2018. № 9. С. 96–102.
2. Городов О. А. Основные направления совершенствования правового регулирования в сфере цифровой экономики в России / О. А. Городов, М. А. Егорова // Право и цифровая экономика. 2018. № 1. С. 6–12.
3. Воронина Н. П. Правовое обеспечение цифровизации сельского хозяйства // Право и цифровая экономика. 2021. № 3. С. 20–26.
4. Рябков Г. О. Электроэнергетика в мире цифровых технологий: правовой аспект / Г. О. Рябков, М. А. Хомякова // Аграрное образование и наука. 2021. № 1. С. 8.
5. Kazakbaev V. Efficiency Analysis of Low Electric Power Drives Employing Induction and Synchronous Reluctance Motors in Pump Applications / V. Kazakbaev, V. Prakht, V. Dmitrievskii, S. Oshurbekov, S. Sarapulov, M. N. Ibrahim // Energies. 2019. T. 12. № 6. P. 1144.

6. Карпухин М. Ю. Автоматизированные гидропонные системы для си-ти-фермерства // Аграрное образование и наука. 2022. № 1. С. 2.

Karpukhin M. Yu. Economic and Energy Efficiency of Potato Cultivation in Different Feeding Areas and the Use of Fungicides in the Middle Urals / M. Yu. Karpukhin, F. Keita // Agrarian Bulletin of the Urals. 2020. № S13. P. 19–23.

7. Старова Е. В. Льготное налогообложение земельных участков, используемых для сельскохозяйственного производства: обзор отдельных арбитражных споров по ставке земельного налога // Вестник арбитражной практики. 2021. № 2. С. 54–60.

8. Колоткина О. А. Оценка правового обеспечения применения информационно-цифровых технологий в агропромышленном комплексе // Российская юстиция. 2020. № 6. С. 51–52.

9. Ягофарова И. Д. Теоретико-методологические подходы к правовому обеспечению трансформации агропромышленного комплекса в условиях цифровизации // Государственная власть и местное самоуправление. 2019. № 11. С. 11–15.

10. Клычова Г. С. Формирование социальной отчетности в органическом животноводстве / Г. С. Клычова, А. Р. Закирова, А. Р. Юсупова, И. М. Хайруллина // Международный бухгалтерский учет. 2021. № 3. С. 297–315.

11. Емельянцева В. П. Цифровизация экономики и ее влияние на реновацию институтов гражданского права / В. П. Емельянцева // Журнал российского права. 2021. № 11. С. 36–53.

Е. Л. Касьянова,

кандидат технических наук, доцент

Сибирский государственный университет геосистем и технологий

М. В. Черкас,

аспирант,

Сибирский государственный университет геосистем и технологий

НАУЧНО-МЕТОДИЧЕСКИЕ ОСНОВЫ КАРТОГРАФИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРАВООЩИТНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Цель исследования – разработка картографического обеспечения правозащитной деятельности, которое может быть представлено в виде традиционных (бумажных) карт, веб-карт и приложений для геоинформационной системы (ГИС) правовой защиты (например, ГИС Уполномоченного по правам человека). В статье представлены тематические карты, предназначенные для правозащитной деятельности, созданные с применением современных компьютерных технологий. При создании карт обращений граждан к Уполномоченному по правам человека Новосибирской области применялось ПО QGIS.

Ключевые слова: право, цифровые технологии, картографическое обеспечение, тематические карты, уполномоченный по правам человека

SCIENTIFIC AND METHODOLOGICAL FOUNDATIONS OF CARTOGRAPHIC SUPPORT OF HUMAN RIGHTS ACTIVITIES

Abstract. The purpose of the study is to develop cartographic support for human rights activities, which can be presented in the form of traditional (paper) maps, web maps and applications for GIS of legal protection (for example, GIS of the Commissioner for Human Rights). The article presents thematic maps designed for human rights activities, created using modern computer technologies. When creating maps of citizens' appeals to the Commissioner for Human Rights of the Novosibirsk region, QGIS software was used.

Keywords: law, digital technologies, cartographic support, thematic maps, commissioner for Human Rights

Тематическое картографирование дает возможность показывать разную информацию в наглядной форме. Картографические способы изображения максимально подробно могут передать характер размещения объектов и явлений, их сущность.

Во многих сферах деятельности карты уже стали привычным отображением информации. Пожалуй, правозащитная деятельность не достаточно охвачена передачей наглядной информации с помощью карт. Только в некоторых картографических приложениях геоинформационных систем отражаются компоненты правовой защиты.

Правозащитная деятельность представляет собой интеграцию всех форм активности государственных и негосударственных структур, формальных и неформальных организаций, внутри государственных и международно-правовых институтов, индивидуальных и групповых, организованных и неорганизованных действий, направленных на защиту прав и свобод человека и гражданина от нарушений и посягательств [1]. Правовые основы правозащитной деятельности – это совокупность специальных юридических средств результативного воздействия норм права на регулируемые ими отношения в сфере защиты прав и свобод человека и гражданина [2].

Правозащитные организации – это особый вид негосударственных неприбыльных организаций, деятельность которых направлена на утверждение и защиту прав и свобод человека, эффективный контроль за их соблюдением государством, его органами и должностными лицами. Правозащитные организации содействуют уменьшению организованного насилия, осуществляемого государством.

Для этого они работают одновременно в трех направлениях:

1. Защита прав человека в конкретных случаях (эта помощь должна быть бесплатной для заявителя), общественные расследования фактов нарушений прав человека государственными органами.
2. Распространение информации о правах человека, правовое воспитание.
3. Анализ положения с правами человека [3].

Различные геоинформационные системы, геопорталы, сайты организаций, занимающиеся правозащитной деятельностью, по своей структуре содержат раз-

дела и приложения. В большинстве из них находятся приложения, включающее различные карты и планы.

В Республике Казахстан создана Автоматизированная информационная система «Информационный сервис» Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан - АИС ЕУСС, в котором в целях дальнейшего перехода на безбумажные технологии ведется единый учет заявлений и сообщений о преступлениях, лиц, их совершивших, результатов деятельности органов предварительного следствия, дознания, прокуратуры и судов [4]. Информация, помещенная в АИС ЕУСС постоянно совершенствуется и обновляется. В дальнейшем АИС ЕУСС преобразован в геопортал комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан (рис.1), в котором также представлена статистическая информация на тематических картах. Ведь именно карта может наглядно, точно, в современном виде представить любые статистические данные.

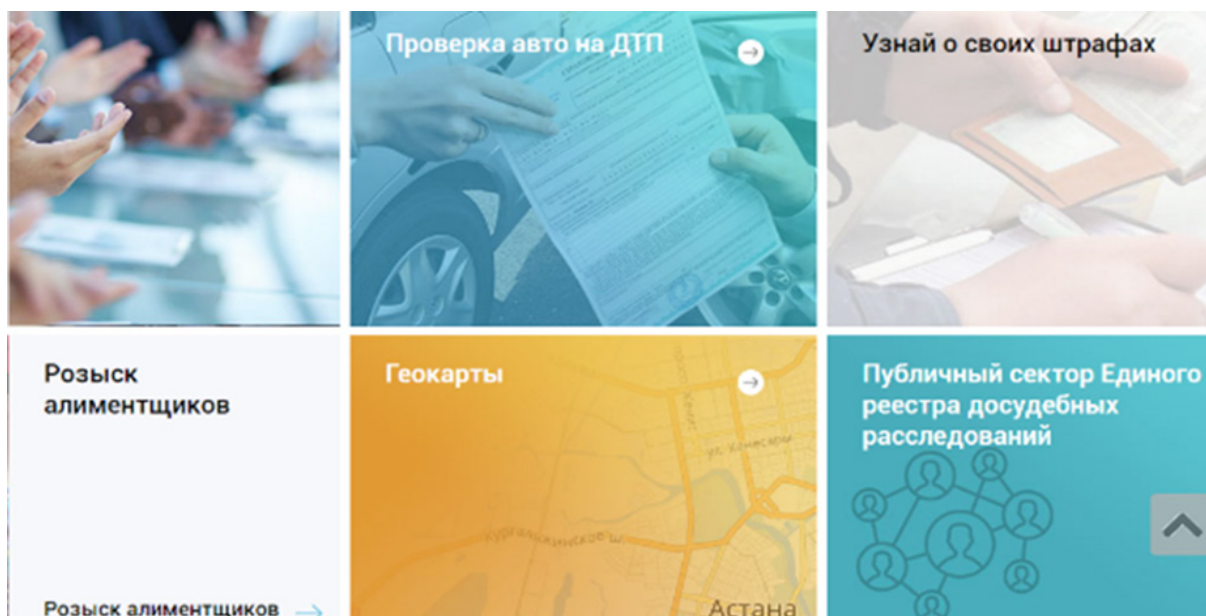


Рис. 1. Структура геопортала комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан

В этом геопортале создан и картографический модуль (рис. 2), где находятся такие карты как: преступности в республике (рис. 3), аварийности в населенных пунктах (рис. 4), преступности в населенных пунктах (рис. 5), преступности несовершеннолетних (рис. 6) и др.

Радует то, что все данные по преступлениям нанесены на карты, но недостаток этих карт, представленных на этих рисунках, в том, что на них используются условные обозначения единые по рисунку для разных объектов и явлений. На одной карте показывается нарушение прав ребенка, а на другой карте теми же способами и знаками нарушение прав женщин.

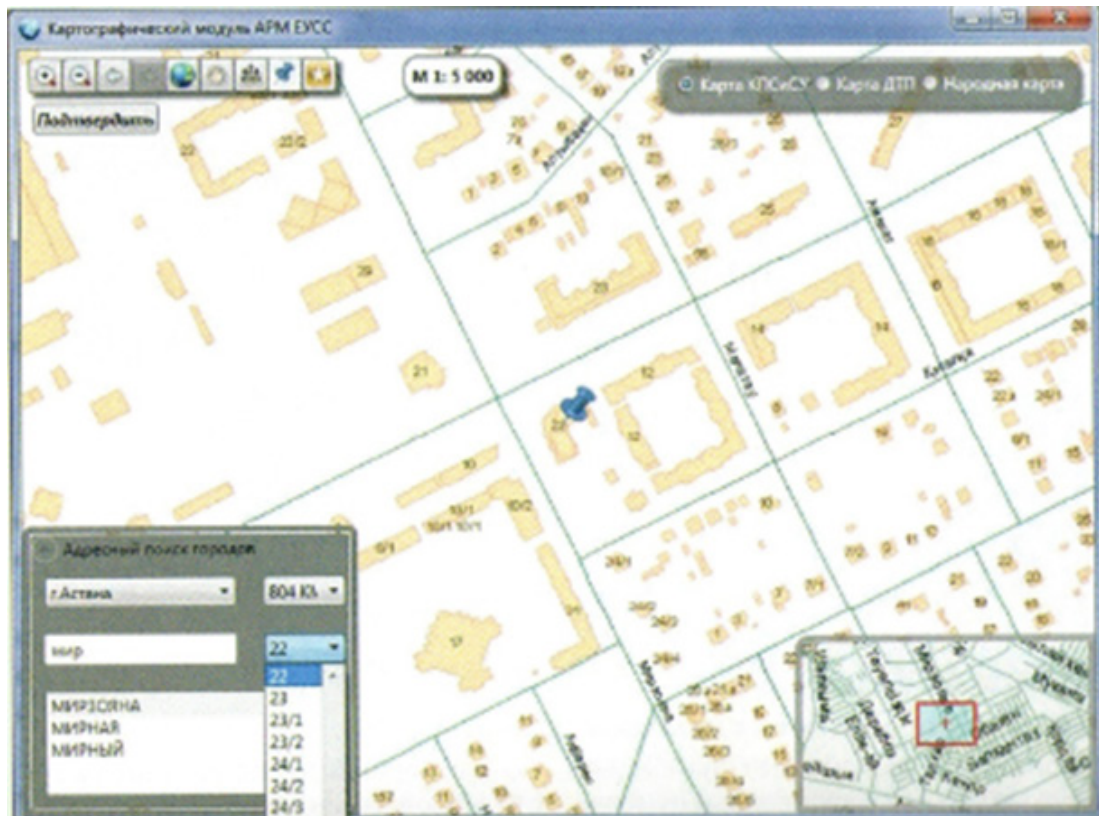


Рис. 2. Картографический модуль



Рис. 3. Карта преступности Республики Казахстан



Рис. 4. Карта аварийности в населенных пунктах



Рис. 5. Карта преступности в населенных пунктах

На карте отображены только те преступления, по которым принято решение о возбуждении уголовного дела и по которым известно точное место совершения преступления. Кроме этого, по желанию любой гражданин может указать на карте место проживания или работы и определенный радиус вокруг этого места, в результате гражданину с указанной им периодичностью на электронный адрес будут приходить сообщения о зарегистрированных преступлениях в его районе.

С правой стороны на панели указан период в рамках которого используются данные о преступности, фильтр (возможность поиска конкретных данных), условные обозначения с указанием количества уголовных правонарушений с ниспадающим списком по конкретным статьям: кража, мошенничество, наркотики, мелкое хищение, самоубийство, хулиганство, грабеж, умышленное причинение средней тяжести вреда здоровью, незаконные изготовление, переработка, приобретение, хранение, перевозка в целях сбыта, пересылка наркотиков, умышленное причинение тяжкого вреда здоровью, изнасилования, нарушение требований пожарной безопасности, нарушение неприкосновенности жилища, присвоение или растрата вверенного чужого имущества, незаконное изготовление оружия, хищение либо вымогательство оружия, боеприпасов, взрывчатых веществ и взрывных устройств и др.

У данного портала достоинства: понятный и доступный интерфейс всего сайта, возможность сразу попасть на другие различные сайты по данной тематике и удобное разделение карт по различным категориям (карты преступности, ДТП и так далее), но есть и существенный недостаток: несколько видов преступлений обозначены одинаковым значком (рис. 8).



Рис. 8 . Единый значок для показа разных видов преступлений

Для каждой конкретной тематической карты необходимо разработать условные знаки, отвечающие конкретной тематике. Каждый условный знак должен отображать конкретный тип объекта.

В настоящий момент карты для правовой защиты разработаны слабо. Карт по тематике преступности в Российской Федерации немного, а выполненных профессиональными картографами, практически нет. В сети интернет можно найти лишь работы, выполненные узкопрофильными специалистами различных правоохранительных структур.

Очень мало информации отображается непосредственно на карте, используя какой-либо один способ отображения, например картограмму, качественный или количественный фон (рис. 9, 10). Статистическая информация показывается на полях карты в виде различных по рисунку диаграммных фигур. К таким картам можно отнести карту «Преступность в России в 2013 году» (рис. 9). Способом количественного или качественного фона? Отображены: наибольшее количество зарегистрированных преступлений (темно-красный цвет) и наименьшее число зарегистрированных преступлений. Остальные данные по видам и количеству преступлений, половозрастным группам лиц, совершающих преступления, показаны способом значков и вынесены на поля карты. Даже эта информация не совсем понятна. Серым и зеленым квадратами показаны тяжкие и особо тяжкие преступления, но не ясно какие из них изображены серым цветом, а какие зеленым.



Рис. 9. Карта «Преступность в России в 2013 году»

Карту «Состояние преступности в России» с натяжкой можно назвать картой, т.к. само картографическое изображение, размещенное в центре, несет мало информации. Способом количественного фона по шкале интервалов (это такая шкала, в которой числа не только упорядочены по рангам, но и разделены определенными интервалами. Особенность, отличающая ее от описываемой дальше шкалы отношений, состоит в том, что нулевая точка выбирается произвольно) изображено количество преступлений. Цветовой фон административных единиц показывает: более 6,9 тыс. преступлений – светло синий цвет, темно синий – от 6,9 до 12,4 тыс., лиловый цвет изображает преступления равные по количеству от 12,4 до 18,6 тыс. Преступность различных видов (основное тематическое содержание) на территории РФ вынесена на поля карты. Художественными значками показаны самые распространенные виды преступлений в РФ: кражи, незаконный оборот наркотиков, экономические преступления, грабежи, незаконный оборот оружия, экологические преступления (рис. 10), но они не размещены на карте и не понятно в каких регионах эти преступления распространены.



Рис. 10. Карта «Состояние преступности в России»

На картах правовой защиты можно передать большое количество статистических данных, сочетая несколько картографических способов отображения.

Кроме традиционных изображений, таких как карты, появилось отображение информации на дашбордах. Это новые инструменты картографической коммуникации. Панели мониторинга – одноэкранные системы визуализации, в которых различные важные элементы информации размещаются на экранных панелях (рис. 11) [9].

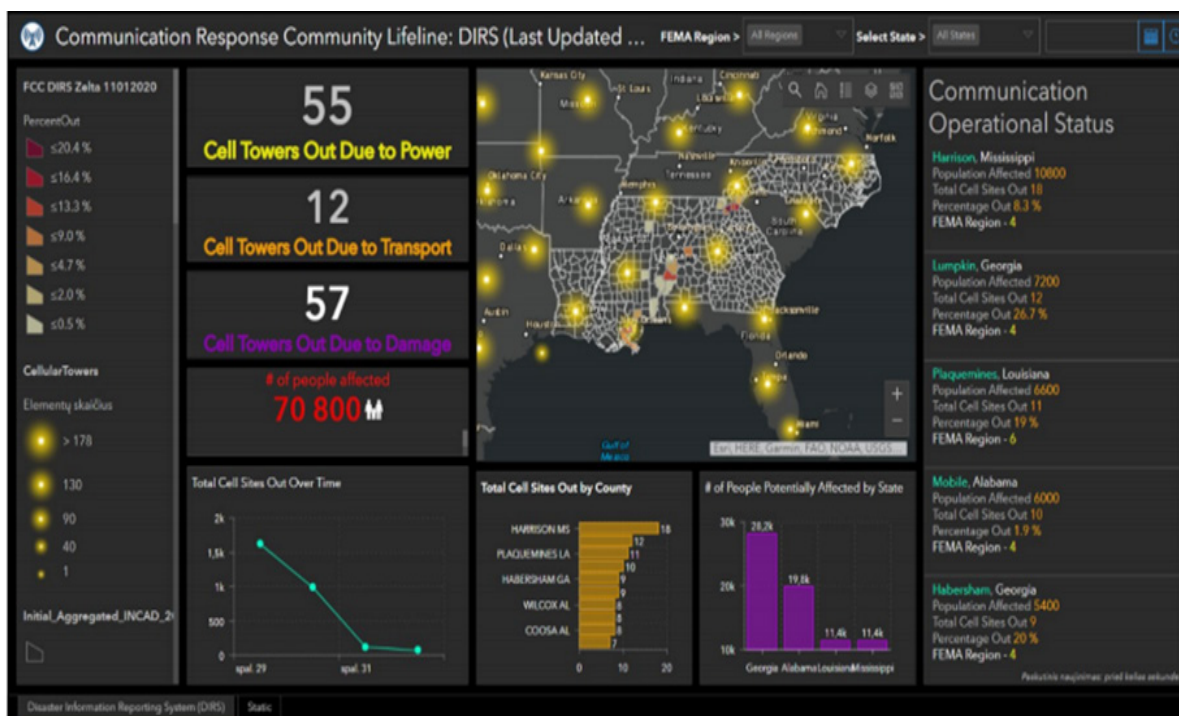


Рис. 11. Пример панели управления с картой, на которой даны типичные элементы (URL 1: Федеральное агентство по чрезвычайным ситуациям, 2021 год)

Такие панели позволяют пользователю получить общий вид на набор данных. Информационные панели могут включать не только текст, диаграммы и графики, но и веб-карты, поэтому их потенциал с точки зрения интерактивной визуализации может быть использован и для картографических задач.

Из-за отсутствия единых условных знаков, показывающих отдельные виды преступлений сложно получать информацию, интересующую правозащитников и других пользователей.

Правильное раскрытие темы картографического произведения должно обеспечить высокий идейный и научный уровень трактовки темы, единство и целостность проектируемого картографического произведения.

Единство и целостность карты предполагают:

- наличие единой концепции отбора ее содержания, основной идеи, посредством которой раскрывается и трактуется на карте ее тема (должны быть показаны все учреждения и организации, занимающиеся правовой защитой);
- наличие взаимосвязей между элементами ее содержания, находящимися в зависимости друг от друга и от целого как взаимодействующего комплекса (показать объекты, в которых могут происходить нарушения прав человека);
- полноту комплекса сравнимых, взаимодополняющих, согласованных элементов и объектов содержания;
- одновременность картографируемых явлений при правильно выбранных хронологических «рамках» или дате;

– единообразие в общем подходе к оформлению всех элементов содержания карты с выделением из них важнейших.

Две ключевые характеристики социального картографирования – это соучастие и аналитический характер. Картографирование нарушений и злоупотреблений в области прав человека направлено на выявление соответствующих факторов, ключевых участников и их взаимосвязей, с тем чтобы определить меры, которые могут быть приняты для улучшения ситуации.

Составлена карта преступности на территорию Кемеровской области, отвечающая всем требованиям, предъявляемым к геоизображениям (рис. 12).

Число зарегистрированных преступлений показано способом картограммы в шкале: менее 300; от 300 – 500; от 500 – 800; более 800. Интенсивность цвета административного района меняется от бледно-голубого (менее 300) до темно-голубого (более 800) в зависимости от показателя.

Количество преступлений в регионе и его виды (в %) изображено способом картодиаграммы (диаграммная фигура показана кругом, разделенным на сектора). Диаметр круга меняется в зависимости от показателя числа зарегистрированных преступлений в районе (менее 300 – 14 мм; от 300 – 500 – 17 мм; от 500 – 800 – 20 мм; более 800 – 23 мм) чем больше показатель, тем больше диаметр круга. Сектора диаграммной фигуры соответствуют виду преступления: убийство – оранжевый, кража – желтый, угон – зеленый, мошенничество – голубой, наркотики – розовый, другие виды – серый.

На полях карты, в качестве дополнительной информации составлены графики столбчатыми диаграммами (уровень преступности показан синим цветом, количество преступлений несовершеннолетними – зеленым цветом):

– преступность по административным районам на 10 000 тысяч человек (в 1 мм – 10 условных преступлений);

– количество преступлений совершенных лицами до 18 лет (в 1 мм – 1 лицо).

Конечно, исходя из задач, связанных с деятельностью правозащитных организаций, необходимо определить общегеографические элементы и тематическое содержание карт, предназначенных для правовой защиты. Такие карты определены как социально-экономические (рис.13) [5, 6] и представлены могут быть в виде цифровой карты, отображаемой картографическим web-сервисом [7]. Веб-карты уже доступны, а их интерактивность позволит не подготовленным в картографии пользователям автоматизировать процесс создания карты [8].

Для Уполномоченного по правам человека (ребенка, предпринимательства и проч.), важно наглядно показать решение вопросов граждан, которые обращаются к Уполномоченному. К сожалению, сейчас на сайте размещена схема районов Новосибирской области (НСО), не показывающая даже населенные пункты, где он был с рабочим визитом (рис. 14). Лучше разместить полноценную административную карту, передающую большое количество информации, используя веб-технологии (рис. 15).

Уполномоченные, назначенные Президентом РФ, решают большое количество разных вопросов граждан. Свою работу они представляют в отчете и было бы очень хорошо и наглядно это делать на картах.

Карта «Преступность Кемеровской области»

1: 4 000 000

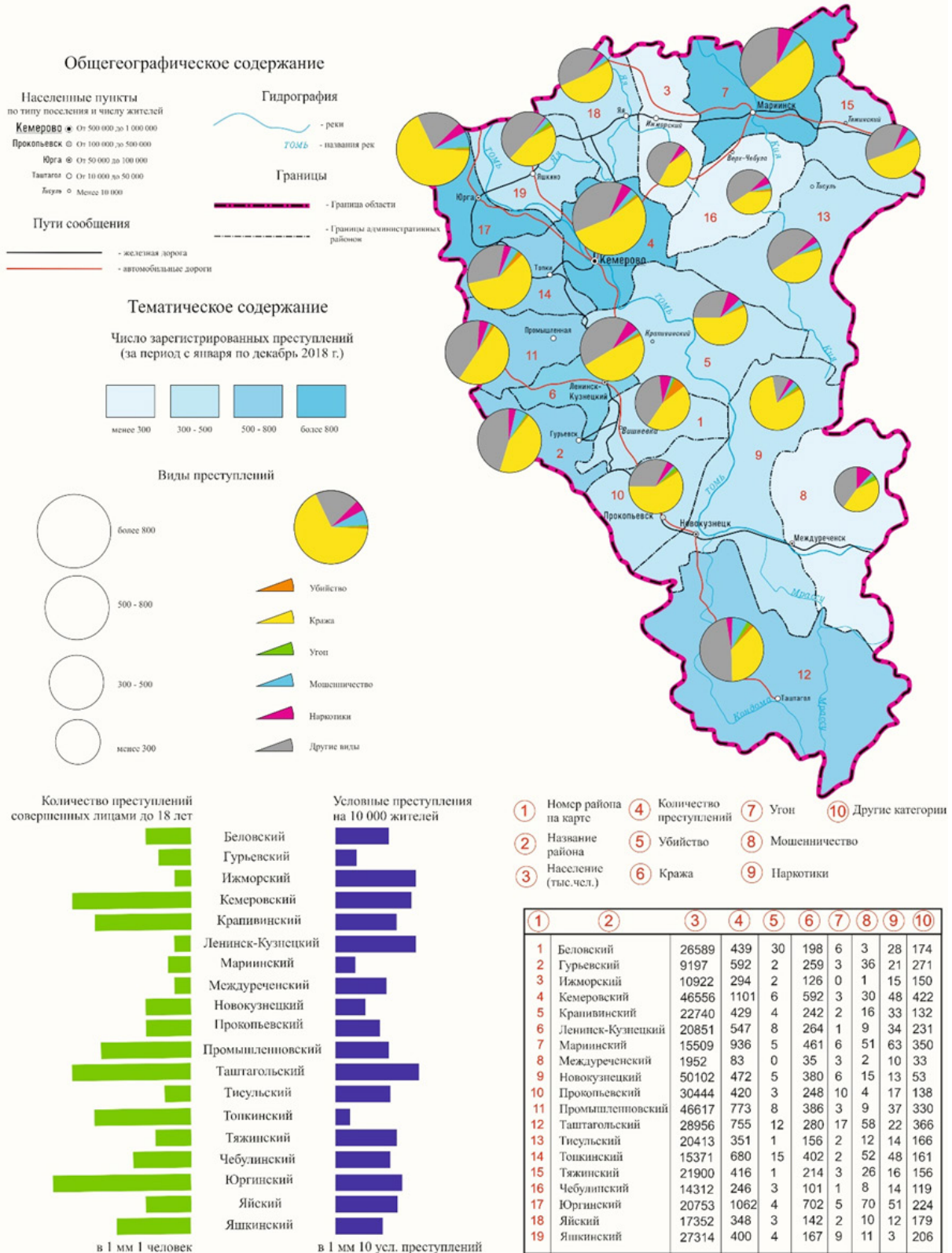


Рис. 12. Карта преступности Кемеровской области



Рис. 13. Место карт правозащитных организаций в классификации тематических карт



Рис. 14. Схема районов Новосибирской области

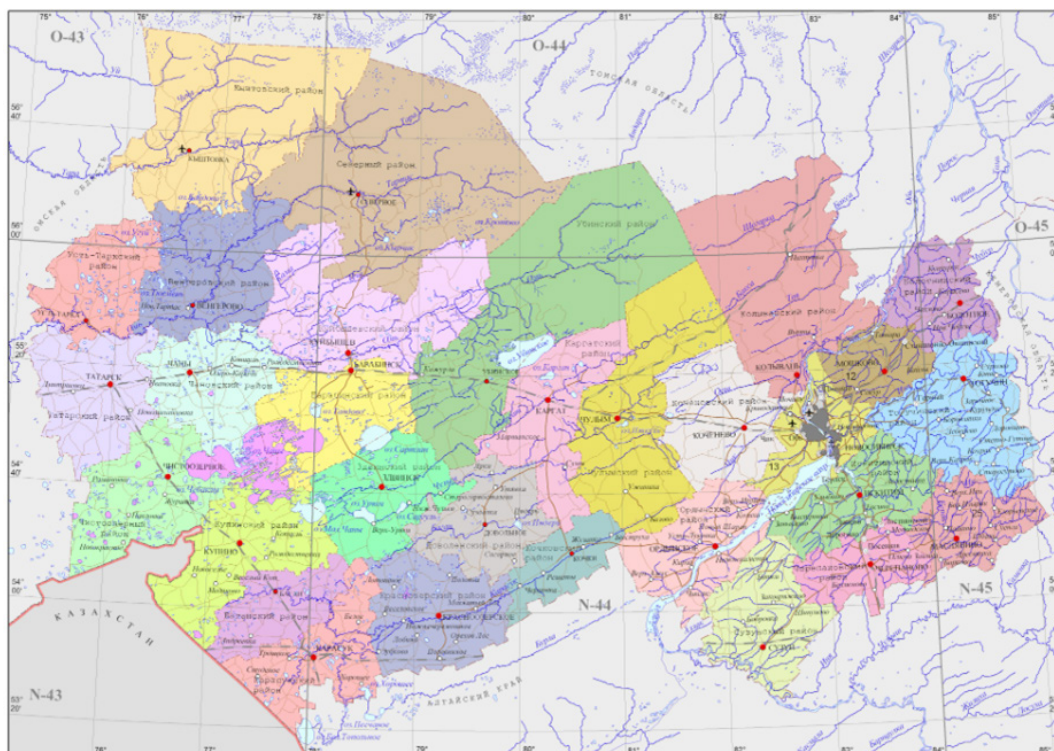


Рис. 15. Административная карта НСО

Тематическая карта на основании данных по количеству письменных обращений граждан за 2019 год к уполномоченному по правам человека составлена для оценки и анализа работы гражданско-правовых обращений. Карта создана в ознакомительных целях, в связи с чем круг пользователей достаточно обширен. Тематика, отображенная на карте, имеет применение как в повседневных делах, так и в научных целях.

Карта составлена в масштаб 1:5000000, в нормальной конической проекции Каврайского.

Географическая основа для нанесения тематического содержания взята с административной карты Новосибирской области. Элементы общегеографической основы: административные границы районов Новосибирской области с их административными центрами районов. Административные центры отмечены красными пунсонами, границы районов показаны сплошными черными линиями. На карте тематическое содержание отображено способом картограммы, районы окрашены в один цвет различной интенсивности в зависимости от показателей. На каждый район рассчитано количество письменных обращений за 2019 год, чем письменных обращений больше, тем темнее цвет района. В тех районах, где отсутствуют письменные обращения окраски территории нет.

Для создания карты использовано ПО QGIS. Версия программы 3.10.14.

Изначально в программу загружались файлы формата shape содержащие объекты полигонального типа, отображающие районы Новосибирской области. Файлы скачивались из сети интернет, для чего использовался запрос: “shape файлы новосибирской области”.

Данные по обращениям к уполномоченному по правам человека прописываются в таблице атрибутов для каждого района в отдельности (рис. 16).

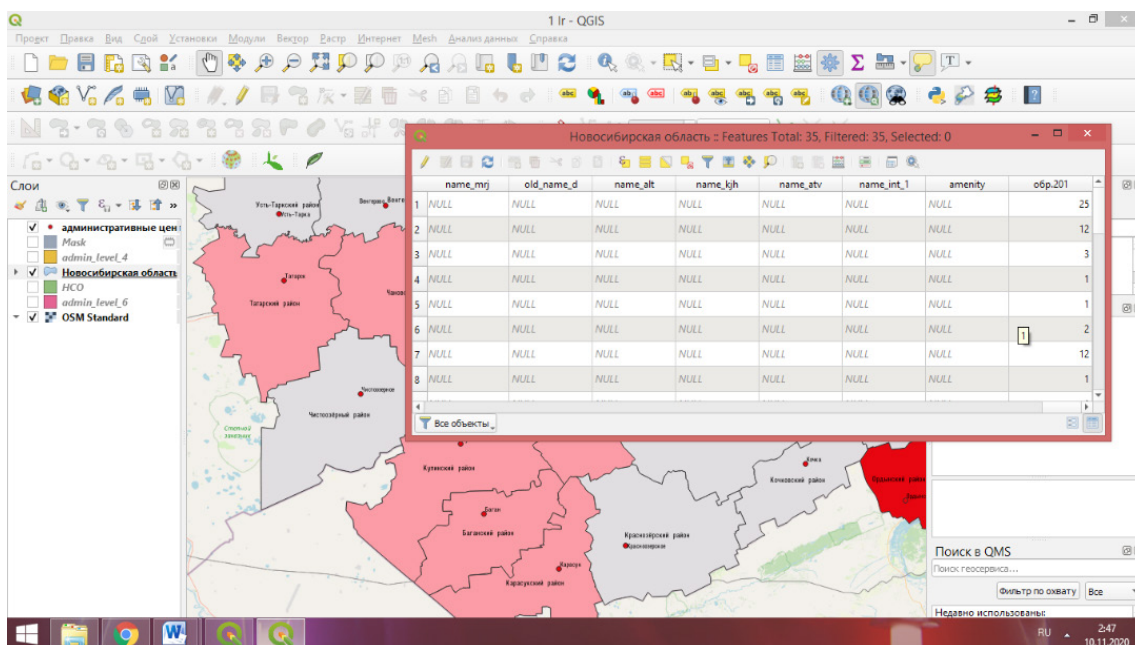


Рис. 16. Внесение данных в таблицу атрибутов

После внесения данных в свойствах слоя следует выбрать стиль отображения, и в его способах выбрать «Уникальные значения». При выполнении классификации (нажатии на кнопку «классифицировать») программа автоматически добавит уникальный цвет каждому значению. Цвета можно настроить, разбив на интервалы и в ручную (рис. 17).

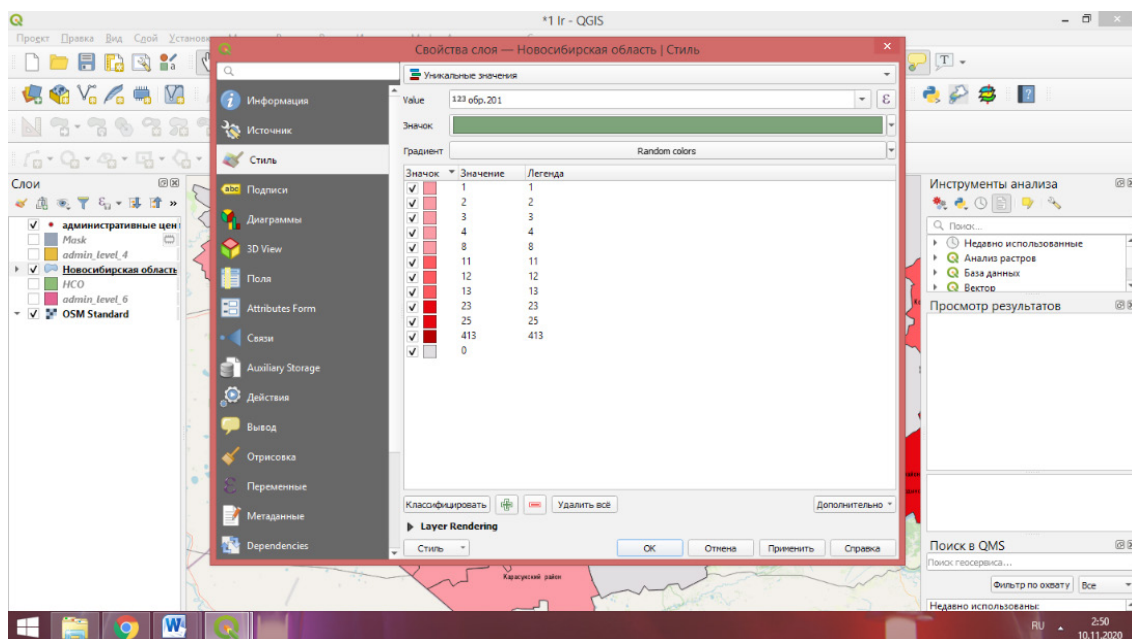


Рис. 17. Открытие стиля отображения данных

После чего нажимается вкладка «ок» и каждый объект на карте окрашивается в присвоенный ему цвет. В параметре «подписи» возможна настройка надписей объектов. Так, например, на карте подписаны административные районы и их центры (рис. 18).

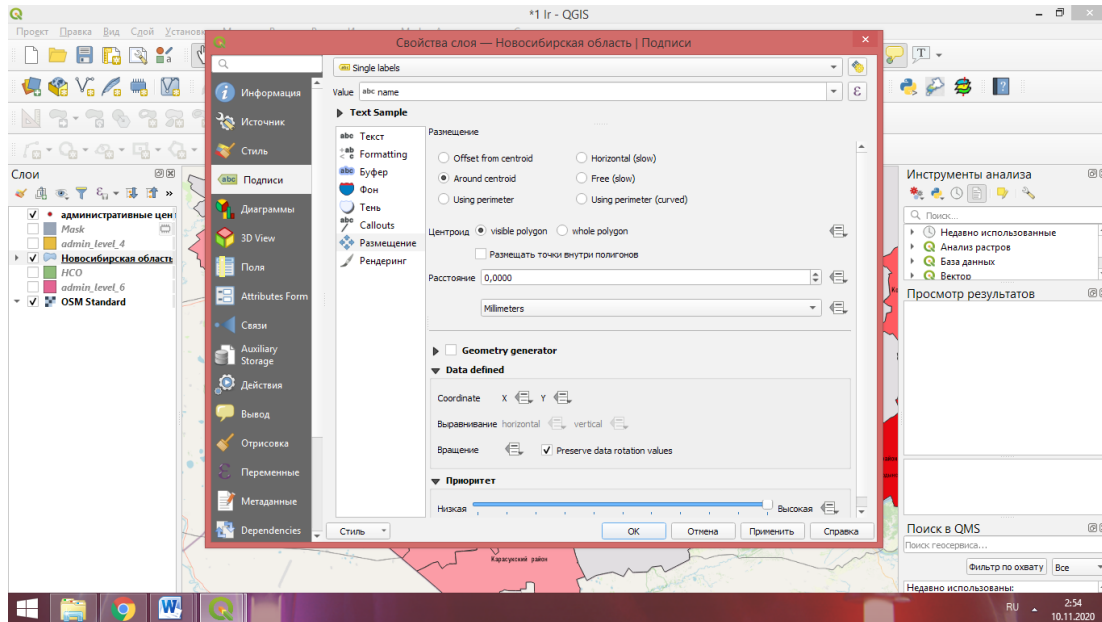


Рис. 18. Настройка надписей

Те же шаги сделаны и в точечном слое, который отображает центры районов. Только в случае с центрами районов в таблицу атрибутов добавляются названия населенных пунктов, после чего выводятся надписи вышеуказанным методом. Точечные объекты можно настроить во вкладке стиль (рис. 19).

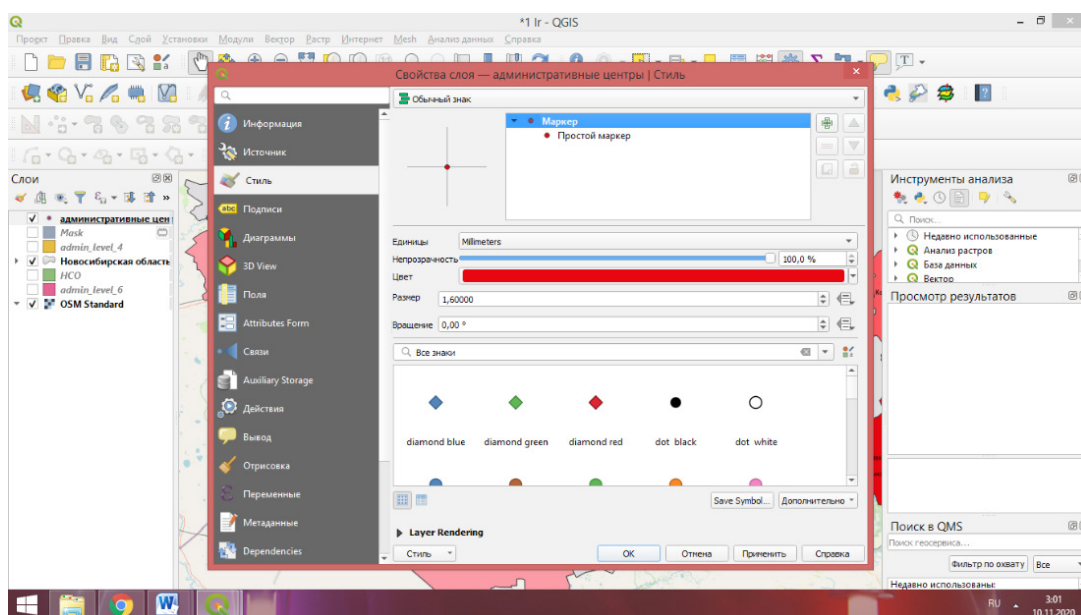
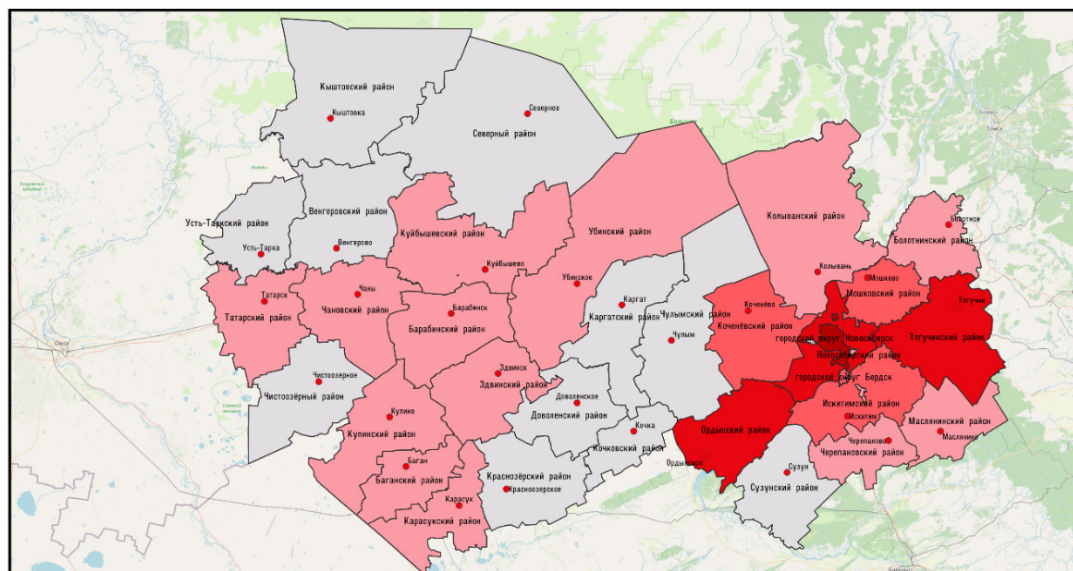


Рис. 19. Настройка стиля отображения точечных объектов

После проведения всех работ создана тематическая карта (рис. 20), которая может быть использована для ГИС Уполномоченного по правам человека Новосибирской области и представлена в его отчете Президенту РФ.

Количество письменных обращений граждан за 2019 год к Уполномоченному по правам человека



Масштаб 1:5 000 000

• Центры районов

Количество письменных обращений граждан за 2019 год

- 1-10 обращений
- 11-20 обращений
- 21-30 обращений
- 31+ обращений
- Обращения отсутствуют

Рис. 20. Тематическая карта, составленная по статистическим данным

Список литературы

1. Алейников Б. Н. Правозащитная деятельность адвоката. Пенза: Изд-во ПГУ. 2017. 96 с.
2. Розенцвайг А. И. Международная правозащитная деятельность. Самара: Изд-во Самарского университета, 2020. 92 с. Закон и правопорядок // Отдел «Правовая защита». URL: <http://zakon.gin.ru>. (дата обращения: 16.06.2021).
3. Автоматизированная информационная система «Единая унифицированная статистическая система» – АИС ЕУСС. URL: <https://arcview.esri-cis.ru/2015/03/03/crime-map-of-kazakhstan/> (дата обращения: 16.06.2019).
4. Ромашова Л. А. Основы тематической картографии: учеб.-метод. пособие / Л. А. Ромашова, О. Н. Николаева. Новосибирск: СГГА, 2013. 86 с.
5. Берлянт А. М. Картография: учебник. М.: КДУ, 2016. 448 с.
6. Дышлюк С. С., Павлов Е. В. К вопросу компьютеризации тематических карт // «ИнтерКарто-ИнтерГИС17» Устойчивое развитие территорий: теория ГИС и практический опыт, 14-15 декабря 2011 г. Белокуриха, 2011. С. 32-36.

7. Касьянова Е. Л., Кикин П. М. Особенности разрабатываемой справочно-аналитической ГИС, возможные области ее применения: сборник материалов IX Международного научного конгресса и выставки «ИНТЕРЭКСПО ГЕО-СИБИРЬ-2013». Новосибирск, 2013. Т. 2, С. 174–182.

8. Касьянова Е. Л., Кикин П. М. Принципы автоматизированного построения тематических слоев: сборник материалов VIII Международного научного конгресса и выставки «ИНТЕРЭКСПО ГЕО-СИБИРЬ-2012». Новосибирск, 2012. Т. 2, С. 105–110.

9. Gružas Kostas Dashboards – new tools of cartographic communication // Institute of Geosciences. Vilnius University. 2020. URL: kostas.gruzas@chgf.stud.vu.lt (дата обращения: 05.05.2021).

И. В. Штепа,

ассистент кафедры экономических дисциплин,
Калининградский институт экономики

Санкт-Петербургского университета управления и экономики

ЛОГИКА И МЕТОДОЛОГИЯ ЦИФРОВИЗАЦИИ НАУКИ: ПРИМЕНИМОСТЬ РАБОТ ПО СИНЕРГЕТИКЕ В СОВРЕМЕННЫХ ИССЛЕДОВАНИЯХ

Аннотация. В статье рассмотрены возможности применения синергетики в теории управления. Особое внимание уделяется использованию синергетики в исследованиях по цифровизации психологии и социологии управления, а также в принятии инвестиционных решений. Проведенное исследование показало, что работы основоположников имеют большое значение для теории управления. Они позволяют по-новому взглянуть на психологические аспекты управления, такие как принятие управленческих решений, мотивация персонала, поведение сотрудников, восприятие ими управленческого воздействия и новой информации, поступающей из внешней среды, этику управления.

Ключевые слова: цифровизация науки, синергетика, психология, социология, инвестиции, теория управления, инновационная деятельность

LOGIC AND METHODOLOGY OF DIGITALIZATION OF SCIENCE: APPLICABILITY OF WORKS ON SYNERGETICS IN MODERN RESEARCH

Abstract. The article discusses the possibilities of using synergetics in management theory. Particular attention is paid to the use of synergetics in research on the digitalization of psychology and sociology of management, as well as in making investment decisions. The conducted research showed that the works of the founders are of great importance for the theory of management. They allow you to take a fresh look at the psychological aspects of management, such as managerial decision-making, staff motivation, employee behavior, their perception of managerial impact and new information coming from the external environment, ethics.

Keywords: digitalization of science, synergetics, psychology, sociology, investments, management theory, innovation activity

Введение. Синергетическая идея процессов самоорганизации и сверхсложных систем сформировалась на основе изучения термодинамических процессов неравновесности и была развита физиками и математиками И. Пригожиным, Г. Хакеном, С. Курдюмовым и др. В первых теоретических работах высказывалось убеждение, что синергетическая закономерность имеет неделимый характер, она распространяется и на другие уровни существования природы, а также на социокультурные процессы.

Управление, по мнению К.Х. Делокарова [1. С. 26-28], требует знания свойств управляемой системы. Поэтому он начинает собирать информацию о состоянии управляемой системы, ее связях и логике ее работы. Полученная информация является основой для формирования консультативной группы. После подачи команды на управление той или иной системой следующий процесс должен протекать по определенному шаблонному алгоритму.

На наш взгляд, по большей части значение для теории управления [14. С. 136-144; 15. С. 173-176] имеют работы основоположников синергетики (И. Пригожина, Г. Хакена, С. Курдюмова, Е. Князевой), внесших значительный вклад в развитие этой теории. Они дают по-новому взглянуть на управление, психологию и социальное управление, деятельность компании как самоорганизующейся структуры, ее экономический рост и инновационное развитие. В организационной структуре возникает синергетический эффект, который, как отмечает Г. Форд, «в сложном коллективе достигается за счет групповой компенсации специальных неспособностей» [10. С. 18]. Таким образом, использование синергетики в науке управления, на наш взгляд, будет способствовать разработке продуктивных методов управления производством и людьми, созданию новой системы управления, ориентированной на развитие.

Синергетика и психология управления. С позиции Г. Хакена [12. С. 16] синергия начинается с наблюдения, что поведение многих систем сильно зависит от условий. Параметры управления навязываются системе извне. В некоторых случаях некоторые параметры управления задаются внутри, но ведут себя так, как если бы они устанавливались извне. Стратегия синергии следующая: она рассматривается уже с известного состояния системы, с заданными значениями параметра. Если будет изменение нескольких параметров, система может стать нестабильной.

Г. Хакен применил синергию к общим идеям групповой терапии, в частности, для перцептивных и поведенческих процессов, где мозг рассматривается как гигантская синергетическая система. По его мнению [12. С. 16], есть равноправие подходов к познанию и поведению. Другими словами, можно начать рассматривать понятия через словесные представления. Так что попробуйте облечь эти понятия в математическую формулу и доказать полезность этих понятий при моделировании процессов на компьютере, а потом уже можно пробовать строить произведения или даже автономные объекты. По словам Г. Хакена, синергетика связана в осуществлении первых трех шагов. Им был разработан своеобразный «синер-

гетический компьютер», который был осуществлен на основе реальных компьютеров. Он основан на трех компонентах распознавания образов. Распознавание образов означает действие механизмов оперативной памяти. Ассоциативная память реализуется динамическим путем и процесс распознавания образов понимается как процесс формирования образов. Таким образом, по словам Г. Хакена [11. С. 16], синергетический компьютер может распознавать не только лица, но и выражения лиц, т.е. эмоции, заниматься изучением двойственных изображений, анализировать сцены и обучаться.

При таком подходе, по мнению Г. Хакена [11. С. 18–26], наше прошлое состояние исходит из нашего опыта и, возможно, также из снов о себе. Согласно теории хаоса, ожидаемое будущее может сильно отличаться от истинности с течением времени. Таким образом, снова и снова должны происходить некоторые корректировки, когда мы воспроизводим ситуации, которые уже были пережиты. Обобщить всю эту картину можно, если опираться на опыт других людей, их представления о прошлом, а затем экстраполировать этот опыт на будущее. Так, по мнению Г. Хакена [11. С. 18–26], будущее, которое мы конструируем в нашей голове, представляет собой сдвинутое во времени прошлое, но здесь возможен шаг вперед в том смысле, что не только любой из нас подвержен влиянию других людей, наоборот. Это приводит к коллективному принятию решений.

На наш взгляд, такой подход важен при изучении психологии управленческих решений. Процесс принятия управленческих решений также ориентирован на прошлый опыт и решение может быть более эффективным либо обобщение чужого опыта, коллективное принятие решений. Для этого, на наш взгляд, целесообразно использовать метод «мозгового штурма» и синергии, что способствует более эффективному поиску и генерации новых идей, согласованию мнений нескольких лиц на основе личного и профессионального опыта каждого и, тем самым принимая продуктивные решения.

Е. А. Евтюхина в статье «Синергетика и психологическая связь» [3. С. 11] исследовала использование синергетического подхода в системе документальной коммуникации. После анализа сущностных основ системы документооборота О. П. Коршунов сформулировал положение о психологической связи в виде концепции теории информации в зависимости от того, где в психике человека находится информационное явление на всех структурных уровнях его обучения. Согласно исследованию, психологическая связь имеет трехуровневую структуру, в основе которой лежит трехуровневая структура психики человека, представленная в новейшем домашнем труде по психологии.

На наш взгляд, синергетический подход к изучению системы информационного взаимодействия может быть применен и в управленческой психологии при изучении процессов восприятия руководством организации и работниками информации, поступающей из внешней среды, процессов взаимодействия между работниками и отдельными лицами. трудового коллектива, а также документальное общение между многочисленными структурными подразделениями. Это будет способствовать более продуктивному использованию информационных и человеческих ресурсов, снижению затрат в многочисленных структурных подразделениях и т. д.

М. Улановский в статье «Синергетическая метафора сознания» [9. С. 18] описал действие феномена флуктуации, предложенного Е.Н. Князевой и С. П. Курдюмовым, и принцип порядка из хаоса, предложенный И. Пригожиным, применительно к человеческому сознанию. Как отмечают Е.Н. Князева и С. П. Курдюмов, из отличительных черт систем, проявляющих нелинейное поведение, является то, что блуждают по возможностям поля [6. С. 24]. Флуктуации – случайное колебание приближенной определенной стадии развития является важной основой нелинейных систем. Этот феномен связан с его гибкостью и приспособляемостью, способностью к непредсказуемым изменениям (10).

Синергия также важна в социологии управления. По мнению Е. А. Князевой и С. П. Курдюмова [5. С. 25], синергизм свидетельствует о том, что пути его развития нельзя навязывать сложным системам. Вместо этого нам нужно понять, как внести свой вклад в наши тенденции развития. Проблема управляемого развития принимает форму проблемы саморазвития.

По утверждению К. В. Харченко [12. С. 16], синергетический подход в социологии предполагает понимание общества как организма, который развивается по собственным законам функционирования, выживания и развития. Задача социальной синергетики состоит в том, чтобы определить условия и факторы постоянного развития общества. Формирование механизмов самоорганизации, по его мнению, возможно за счет воздействия на ноосферу (концепция В.И. Вернадского). В понятие ноосфера входят информационные потоки и коммуникативные действия, образующие совокупность общечеловеческих действий и представлений. Благодаря коммуникационным связям происходит синтез структур общества. эволюционное развитие. Реализуется на основе информационного обмена, определяет естественный выбор энергетически выгодных форм общества.

Согласно мнению К.Х. Делокарова [1. С. 30–32], общественное образование – фирма, завод, сектор в НИИ и т. п. – это не механическая сумма индивидуумов, составляющих это образование. Как отмечал Э. Дюркгейм: «...общество есть не простая сумма индивидов, а система, образованная их союзом, представляющая действительность... наделенная своими особенностями». Любое сообщество, объединившееся для решения проблемы, естественно, содержит определенное количество противоречий и даже конфликтов. И хотя людей объединяют общие мотивы, интересы и цели, в процессе решения определенных задач они могут самостоятельно интерпретировать ход их выполнения. Успех компании, ее стабильность, стабильность работы во многом зависят от руководителя. В обществе, по мнению К. Х. Делокарова значит работать с людьми и для людей, что предполагает знание людей, их желаний, мотивов и устремлений. Как отмечают С. П. Курдюмов, Г. Г. Малинецкий, А. Б. Потапов в своей работе «Синергия – новые направления» во многих случаях пытаются управлять системой, не зная ее внутренних свойств и навязывая желаемое поведение, что не только бесполезно, но и опасно. Управление может быть основано только на знаниях. Поэтому с позиции К. Х. Делокарова [1. С. 22–24], можно сказать, используя синергетический язык, что управление по сути есть способность оптимально взаимодействовать с усилиями знающих предмет людей, поскольку проблемы сотворчества импли-

цитно проявляются в процессе управления. Или явно обновляется, возможность поработать людей, выполняющих определенную задачу, чтобы ваш внутренний набор задач был решаемым. Исходя из этого, управление можно определить как разделение функций по координации усилий. На наш взгляд, в отношении внутрифирменного управления необходимо делегировать полномочия от руководителя специалистам того или иного профиля. Создание специализированных структурных подразделений, согласованная направленность их работы, взаимосвязи между ними (например, в инновационных компаниях, занимающихся разработкой и внедрением новых технологий могут быть взаимосвязи между ИТ-центром и отделом совершенствования технологий). Кроме того, на наш взгляд необходим индивидуальный подход к каждому работнику с учетом его специфических предпочтений, влияющих на мотивационное стимулирование.

Синергия и теоретические аспекты управления инвестициями. Синергетические трактовки предпосылок социально-экономических процессов поддерживаются от основоположников от современной общей теории самоорганизации И. Пригожина и Г. Хакена. И. Пригожин и И. Стенгерс дают ответ на вопрос, распространяется ли синергетическая аналогия на области, где термодинамика не может играть ведущей роли. Представленные данные показывают важность спонтанности возникновения событий, нелинейных проявлений экономической активности, в том числе инвестиционных процессов, которые могут быть решены в контексте синергии [9. С. 18].

Такие процессы, как возникновение и развитие идеи социально-экономической самоорганизации, по мнению О. С. Сухарева, С. Шманева, А. М. Курьянова, являются ярким примером познанием и созданием новых направлений научной деятельности. Недостатки управления сверхсложными системами классической парадигмы с нелинейным развитием экономики привело к ее кризису из-за неустойчивости представлении об их развитии.

Заключение. Проведенное исследование показало, что работы основоположников синергетики имеют большое значение для теории управления. Они позволяют по-новому взглянуть на психологические аспекты управления, такие как принятие управленческих решений, мотивация персонала, поведение сотрудников, восприятие ими управленческого воздействия и новой информации, поступающей из внешней среды, этику управления и др., а также на особенности руководства инновационными процессами и творческими личностями, мотивации их к поиску и генерации новых идей, созданию инновационного продукта. Вместе с тем, они рассматривают организацию как самоуправляемую систему, что, на наш взгляд, способствует более эффективному управлению путем делегирования руководителем значительной части своих полномочий профессионалам, имеющим знания и опыт в своем деле.

Список литературы

1. Делокаров К. Х. Синергетика и познание социальных трансформаций // Синергетическая парадигма: человек и общество в условиях нестабильности. М.: Прогресс-Традиция, 2003.

2. Дюркгейм Э. О разделении общественного труда. Метод социологии. М.: Наука, 1991.
3. Евтюхина Е. А. Синергетика и психологическая связь // Библиография. № 2. 2009.
4. Каган М. С. Синергетическая парадигма – диалектика общего и особенного в методологии познания разных сфер бытия // Синергетическая парадигма: нелинейное мышление в науке и искусстве. М.: Прогресс-Традиция, 2002.
5. Князева Е. Н., Курдюмов С. П. Синергетика как новое мировидение: диалог с И. Пригожиным // Вопросы философии. № 12. 1992.
6. Князева Е. Н., Курдюмов С. П. Основания синергетики. Режимы с обострением, самоорганизация, темпомиры. СПб.: Алетейя, 2002.
7. Пригожин И. Философия нестабильности // Вопросы философии. № 6. 1991.
8. Сухарев О. С., Шманев С. В., Курьянов А. М. Синергетика инвестиций: учеб.-метод. пособие. М.: Финансы и статистика, 2008.
9. Улановский А. М. Синергетическая метафора сознания // Вестник Московского Университета: психология. Серия 14. № 1. 2005.
10. Форд Г. Моя жизнь, мои достижения. М.: Финансы и экономика, 1989.
11. Хакен Г. Синергетика и некоторые ее применения в психологии // Синергетическая парадигма: нелинейное мышление в науке и искусстве. М.: Прогресс-Традиция, 2002.
12. Харченко К. В. Социология управления: от теории к технологии. Белгород: Белгородская областная типография, 2008.
13. Шевченко И. В., Дробышевская Л. Н. Инновационная основа смены технологических укладов в современной глобальной экономике // Финансы и кредит. № 35. 2005.
14. Чаплыгин В. Г., Мороз В. Н. Математическое определение эффективности трансфера технологий // Экономика и математические методы. 2020. Т. 56. № 3. С. 136–144.
15. Чаплыгин В. Г. Устойчивость и равновесие, кооперация и координация в глобальном пространстве Дж. Нэш versus Г. Штакельберг // Известия Томского политехнического университета. 2004. Т. 307. № 2.
16. Чаплыгин В. Г., Мороз В. Н. Принятие решений по трансферу технологий в региональном инновационном кластере в условиях неопределенности и риска // Журнал Новой экономической ассоциации. № 1 (53). С. 121–142. DOI: 10.31737/2221-2264-2022-53-1-6
17. Alinezhad A., Khalili J. (2019) New Methods and Applications in Multiple Attribute Decision Making (MADM) // International Series in Operations Research & Management Science. Vol. 277. Cham: Springer Nature Switzerland AG. 233 p.
18. Ashofteh P.-S., Golfam P., Loáiciga H.A. (2020) Evaluation of River Water Transfer Alternatives with the TODIM Multi-Criteria Decision Making Method // Water Resources Management . Vol. 34. № 15. Pp. 4847–4863.
19. Davoudabadi R., Mousavi S.M., Mohagheghi V. (2020) A new last aggregation method of multi-attributes group decision making based on concepts of TODIM,

WASPAS and TOPSIS under interval-valued intuitionistic fuzzy uncertainty // Knowledge and Information Systems. Vol. 62. № 4, 1371–1391.

20. Eslami V. et al. (2021) Multi-criteria Decision-making Approach for Environmental Impact Assessment to Reduce the Adverse Effects Of Dams // Water Resources Management. DOI: 10.1007/s11269-021-02932-1

21. Egorov N. et al. (2021) Innovative Development in Northern Russia Assessed by Triple Helix Model // International Journal of Technology. Vol. 12. № 7, 1387–1396.

22. Fernández-Serrano, J., Martínez-Román, J.A., Romero, I. (2019) The entrepreneur in the regional innovation system. A comparative study for high- and low-income regions // Entrepreneurship and Regional Development. Vol. 31. № 5–6, 337–356.

23. Krylovas A., Kosareva N., Dadelo S. (2020) European countries ranking and clustering solution by children's physical activity and human development index using entropy-based methods // Mathematics. Vol. 8. № 10, 1–22.

24. Li J., Fang H., Song W. (2019) Failure Mode and Effects Analysis Using Variable Precision Rough Set Theory and TODIM Method // IEEE Transactions on Reliability. Vol. 68. № 4, 1242–1256.

25. Li M.-Y., Cao P.-P. Extended TODIM method for multi-attribute risk decision making problems in emergency response // Computers & Industrial Engineering. Vol. 135, 1286–1293.

26. Luo Y. et al. (2021) Tourism Attraction Selection with Sentiment Analysis of Online Reviews Based on Probabilistic Linguistic Term Sets and the IDOCRIW-COCOSO Model // International Journal of Fuzzy Systems. Vol. 23. № 1, 295–308.

27. Pala O. (2021) Financial performance analysis of BIST transportation companies based on IDOCRIW and MARCOS // Kafkas University, Journal of Economics & Administrative Sciences Faculty. Vol. 12. № 23, 263–294.

28. Sarraf F., Neyad S.H. (2020) Improving performance evaluation based on balanced scorecard with grey relational analysis and data envelopment analysis approaches: Case study in water and wastewater companies // Evaluation and Program Planning. Vol. 79, 1–11.

29. Sharaf, I.M., Khalil, E.A.-H.A. (2020) A spherical fuzzy TODIM approach for green occupational health and safety equipment supplier selection // International Journal of Management Science and Engineering Management. P. 1–13. DOI: 10.1080/17509653.2020.1788467

30. Wang L., Wang Y.-M., Martínez L. (2020) Fuzzy TODIM method based on alpha-level sets // Expert Systems with Applications. Vol. 140, 1–15.

31. Wu W., Xu Z. (2020) Hybrid TODIM Method with Crisp Number and Probability Linguistic Term Set for Urban Epidemic Situation Evaluation // Complexity. Vol. 2020, 1–11.

32. Zhang W., Du J., Tian X. (2018) Finding a promising venture capital project with TODIM under probabilistic hesitant fuzzy circumstance // Technological and Economic Development of Economy. Vol. 26. № 5, 2026–2044.

Т. В. Щукина,

доктор юридических наук, доцент,
заведующий кафедрой прикладного права,
Российский технологический университет – МИРЭА;
ведущий научный сотрудник,
Институт государства и права РАН

ВОПРОСЫ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА РОССИИ: ПУБЛИЧНО-ПРАВОВЫЕ АСПЕКТЫ

Аннотация. Статья посвящена исследованию вопросов становления технологического суверенитета России от импортозамещения к формату самостоятельного устойчивого развития современного научно-технологического уклада вне зависимости от сетевого взаимодействия с другими странами и транснациональными промышленными гигантами. Цель исследования заключается в сравнительно-правовом анализе сущности санкционной политики в отношении Российской Федерации и объективного ответа последней на искусственно создаваемые экономические ограничения с помощью нормативного правового регулирования этих процессов, создания научно-технологической экосреды университетских кампусов и промышленных консорциумов. Задачи исследования также направлены на фиксацию формирования серьезной научно-технологической политики, способной отвечать на возникающие внешние вызовы и нивелировать создаваемые риски. Актуализируется вопрос о роли науки и образования как народной дипломатии в экспорте образования в дружественные страны.

Ключевые слова: технологический суверенитет, импортозамещение, научно-технологическая среда университетских кампусов, экспорт науки и образования

QUESTIONS OF TECHNOLOGICAL SOVEREIGNTY OF RUSSIA: PUBLIC LAW ASPECTS

Abstract. This article is devoted to the study of the formation of technological sovereignty of Russia from import substitution to the format of independent sustainable development of modern scientific and technological structure, regardless of network interaction with other countries and transnational industrial giants. The purpose of scientific research is the comparative analysis of the essence of the sanctions policy in relation to the Russian Federation and the objective response of our country to the artificially created economic restrictions using the normative legal regulation of these processes, the creation of scientific and technological edition of university campuses and industrial consortians. The objectives of the study are also aimed at fixing the formation of a serious scientific and technological policy that can respond to the emerging external challenges and level the created risks. The author actualizes the question of the role of science and education as folk diplomacy in the export of education to friendly countries.

Keywords: Technological sovereignty, import substitution, scientific and technological environment of university campuses, export of science and education

Введение. Вопросы технологического суверенитета России в активном формате стали возникать, начиная с 2014 года после введения экономических и политических санкций в отношении российского государства со стороны европейских государств и США, международных организаций и банковских структур. Санкции и ограничение сотрудничества с Российской Федерацией выразились в широкомасштабном систематическом установлении, а впоследствии расширении перечня мер, влияющих на экономическую изоляцию страны. Это закрепление списков физических и юридических лиц, попадающих под санкции, прекращение финансирования проектов Европейским инвестиционным банком и другими международными финансовыми институтами, фиксация запретов на покупку товаров, включая углеводороды, на поставку техники, оборудования и технологий для отдельных сфер промышленности и другие [1].

Российская Федерация путем проведения последовательной финансово-налоговой политики и развития импортозамещения к 2020 году преодолела санкционное давление и показала: позитивный экономический рост до 2,1%, а совокупный фискальный импульс по бюджетной системе составил 8% ВВП [2]; увеличение золотовалютных резервов, снижение безработицы. «За шесть лет в ряде отраслей, таких как тяжелое, нефтегазовое и пищевое машиностроение - доля отечественной продукции возросла на 15-25%» [3].

В науке в 2014-2015 годах появился термин «экономика импортозамещения», который позволил ученым прогнозировать возможные риски для российской экономики, выявлять слабые места реализации стратегии импортозамещения, определять ключевые сегменты экономики, где возможно добиться замещения импортных товаров и продуктов отечественными. Блохин К.А., Шурухина Т.В. отмечали в тот период времени, что «необходимы: диверсификация импортных источников, снижение зависимости России от импортных информационных технологий; укрепление машиностроения, сельскохозяйственного производства» и формирование иного инвестиционного механизма финансирования предпринимательских проектов [4. С. 131-138].

Политика импортозамещения дала свои определенные результаты и к 2020 году Россия переходит к концепции «не ускоренного импортозамещения, а стимулирования экспорта» [5. С. 88-93]. Отдельные авторы называют подобный экономико-политический процесс «инновационным импортозамещением, под которым понимают снижение импортозависимости, преодоление нехватки импортных товаров путем целенаправленных мер со стороны государства и предприятий МСП, производящие продукцию на российском рынке и использование результатов НИОКР» [6. С. 177-188].

Импортозамещение регулируется государством на правовом уровне, начиная с 2014 года. Был принят ряд нормативных правовых актов в области импортозамещения, их базовой частью стало Постановление Правительства РФ от 15 апреля 2014 года № 328 «Об утверждении государственной программы Российской Федерации «Развитие промышленности и повышение ее конкурентоспособности» [7]. Государственная программа Российской Федерации «Развитие промышленности и повышение ее конкурентоспособности» предназначена для

«объединения усилий государства в сфере развития промышленного потенциала, создания системных долгосрочных стимулов для повышения конкурентоспособности российских промышленных компаний на внутреннем и мировом рынках» [7]. Основопологающей задачей программы выступило «обеспечение технологического развития отечественной промышленности на основе создания и внедрения прорывных, ресурсосберегающих, экологически безопасных промышленных технологий» [7]. Еще в 2014 году государство задумывалось о производстве конкурентоспособной наукоемкой российской продукции.

Основная часть. Впоследствии в развитие общих начал вышеуказанной государственной программы появилось Постановление Правительства РФ от 31 июля 2015 г. № 779 «О промышленных кластерах и специализированных организациях промышленных кластеров» [8]. Промышленные кластеры представляют собой инновационные площадки, объединяющие промышленные предприятия, создающие технологически новую продукцию в сфере машиностроения, новых композитных материалов и других отраслях промышленности, заменяющую импортные компоненты. Приоритетное значение создания промышленных кластеров состояло в том, что объединение предприятий проходило по инициативе самих промышленников; объединялись предприятия, создающие продукцию в единой производственной цепочке; территориально они должны были находиться либо в одном субъекте РФ, либо в близлежащих регионах. Сам же промышленный кластер представляет собой публичное юридическое лицо (специализированную организацию промышленного кластера) с участием конкретного субъекта РФ, который обеспечивает организационную, инфраструктурную, консультационную поддержку предприятий - участников. Без регистрации специализированной организации промышленного кластера и включения промышленного кластера в реестр Минпромторга кооперация промышленных предприятий на основе гражданско-правового договора (соглашения об участии) и их последующая совместная производственная деятельность невозможны. Подобная позиция государства связана с конкретизацией для промышленных предприятий направлений производства продукции и ее видов, а также субсидированием со стороны Министерства промышленности и торговли Российской Федерации ее выпуска (максимальная величина государственной поддержки составляет 1 млрд.рублей).

Постановление Правительства РФ от 28 января 2016 г. № 41 «Об утверждении Правил предоставления из федерального бюджета субсидий участникам промышленных кластеров на возмещение части затрат при реализации совместных проектов по производству промышленной продукции кластера в целях импортозамещения» установило порядок и назначение предоставления субсидий предприятиям – участникам промышленных кластеров. Субсидии «предоставлялись с целью стимулирования производственной кооперации участников промышленных кластеров, а также создания и развития российских производителей сырья, материалов и комплектующих, необходимых для усиления локализации производства конечной промышленной продукции промышленных кластеров на территории Российской Федерации» [9]. Промышленный кластер определяют еще как инструмент территориального промышленного развития на среднесрочный период

(до 8 лет). На 2020 год промышленные кластеры были созданы или создавались в 38 субъектах РФ. В качестве примера приведем такие кластеры как «Кластер Биофармацевтики» (Белгородская область), «Промышленный кластер станкостроения и станкоинструментальной промышленности «ЛИПЕЦКМАШ»» (Липецкая область), «Воронежский областной кластер производителей нефтегазового оборудования» (Воронежская область) и другие [10].

Определенной сложностью для предприятий, желающих создать промышленный кластер, является наличие жестких требований к нему со стороны государства (прозрачность деятельности, объем выручки и т.п.), а также не готовность промышленных предприятий создавать и доказывать инновационную составляющую своей продукции. В связи с чем не во всех регионах есть промышленные кластеры, так как предприятия не решаются брать ответственность за выпуск подобной промышленной продукции на себя, включая необходимость эффективной кооперации.

Наряду с развитием промышленных кластеров в 2015 году стали создаваться индустриальные (промышленные) парки. Постановление Правительства РФ от 4 августа 2015 г. № 794 «Об индустриальных (промышленных) парках и управляющих компаниях индустриальных (промышленных) парков» предусмотрело создание индустриального промышленного парка как площадки, предоставляющей возможность предоставления прав владения и пользования земельным участком и (или) строением либо их частью резидентам технопарка, включая объекты инфраструктуры [11].

Индустриальный (промышленный) парк должен соответствовать определенным требованиям: по величине земельного участка от 8 га, к площадям производственных сооружений – от 20 тысяч кв.метров, к видам деятельности резидентов – производство промышленной продукции, к коммунальной и транспортной инфраструктур [12]. Индустриальный (промышленный) парк сдает в аренду земельные участки и сооружения (общепроизводственного назначения) промышленным предприятиям, которые за счет имущественных возможностей парка снижают свои капитальные затраты, могут пользоваться налоговыми льготами.

Создание промышленных кластеров и индустриальных промышленных парков обуславливается Стратегией пространственного развития РФ и схемами территориального планирования.

Следующим направлением трансформации импортозамещения выступили промышленные технопарки. Логическим развитием формата индустриальных (промышленных) парков стали технопарки, что подтверждает вступление в силу Постановления Правительства РФ от 27 декабря 2019 г. № 1863 «О промышленных технопарках и управляющих компаниях промышленных технопарков» [13]. Направлениями функционирования технопарков могут быть: металлургия, станкостроение, тяжелое машиностроение, судостроительная и авиационная промышленность, радиоэлектронная промышленность и другие актуальные отрасли промышленности для импортозамещения [14]. Специализированными видами промышленных технопарков, начиная с 2022 года, являются агробиотехнопарки и экотехнопарки.

Необходимо отметить, что требования к промышленным технопаркам строятся на величине земельного участка от 1 га, объеме площадей зданий (от 5 тыс. кв. м.), назначении этих площадей (наличие на них производственной и технологической инфраструктуры); видах деятельности резидентов, которая заключается не только в производстве промышленной продукции, но и в проведении научных исследований и разработок. Исходя из сути требований, предъявляемых к технопаркам, управляющая компания технопарка в комплексе сдает в аренду имущество, оказывает специализированные услуги и обеспечивает технологическим оборудованием коллективного использования.

Резиденты промышленного технопарка осуществляют один или все виды деятельности: а) промышленное производство, б) научно-техническую деятельность, в) инновационную деятельность в целях освоения производства промышленной продукции и коммерциализации полученных научно-технических результатов [16]. Следовательно, промышленный технопарк обеспечивает возможность научно-технической деятельности и (или) инновационной деятельности резидентов. Объектами технологической инфраструктуры промышленного технопарка выступают: бизнес-инкубатор, инжиниринговый центр, центр коллективного пользования научным оборудованием, центр коллективного пользования опытно-промышленным оборудованием, сертификационный центр, лаборатория, сварий, инновационно-технологический центр, центр прототипирования, центр обработки данных и другие [16].

Сущность промышленной деятельности резидентов технопарков обуславливает многозадачность и комплексное значение последних в российской экономике. Это – создание новых технологических предприятий, размещение уже существующего высокотехнологичного бизнеса, формирование экосреды для производства инновационной импортозамещающей продукции.

Изменение обстоятельств развития российской экономики в 2022 году обусловило еще большее усиление внимания к деятельности технопарков и видам поддержки их резидентов, особенно к молодым технологическим предпринимателям. Субъекты РФ «получают субсидии на финансирование в виде грантов деятельность субъектов малого и среднего предпринимательства, включенных в реестр социальных предпринимателей, или субъектов малого и среднего предпринимательства, созданных физическими лицами в возрасте до 25 лет включительно» [17]. Максимальный размер этого гранта не превышает 500 тыс. рублей, а минимальный размер гранта – не менее 100 тыс. рублей. Для социальных предприятий и молодых предпринимателей, зарегистрированных и осуществляющих деятельность в Арктической зоне, максимальный размер гранта не превышает 1 млн руб.

На 2022 год в 69 субъектах РФ действуют промышленные технопарки. Больше всего промышленных технопарков создано в Свердловской области, Санкт-Петербурге, республике Татарстан, Московской области, Москве, Владимирской области. Промышленные технопарки разноплановы, например: «Карельские продукты», «РотФронт», «Приборостроение», «Андроидная техника», «Астраханский государственный университет», «Ямал» и другие [18]. Отметим, что в перечне

промышленных технопарков помимо промышленных парков, сконцентрированных относительно инновационных промышленных предприятий, присутствуют университеты (Астраханский, Чеченский государственные университеты, БГТУ им. В. Г. Шухова и др.) и Кванториумы. Это промышленные технопарки, опирающиеся на научно-технологическую среду университетов и школ для одаренных детей. Импортозамещение как вектор изменения экономики России становится визитной карточкой и брендом российских университетов и специализированных научно-образовательных центров для школьников.

Все большее значение в деле решения проблем импортозамещения приобретает, как указывалось выше, научно-технологическая включенность в этот процесс университетов и научных организаций. Президент Российской Федерации на ПМЭФ-2022 отметил о необходимости построения полноценного технологического суверенитета России и соответственно технологической экономике. Целостность технологического суверенитета зависит от «развития инженерного образования, трансфера научных разработок в экономику, финансирования высокотехнологических компаний, развития сквозных технологий и цифровой трансформации отраслей промышленности. Целями импортозамещения Президент Российской Федерации назвал не замену и копирование чужих товаров, а создание собственных конкурентных технологий, товаров и сервисов» [19].

Большинство мер поддержки импортозамещения будут сконцентрированы в промышленности. Это – «новые условия работы промышленных кластеров (льготные кредиты на срок до десяти лет со ставкой до 7 %, низкие налоги, субсидиарная поддержка на старте, гарантированный спрос на продукцию за счет контрактов с госкомпаниями) и запуск промышленной ипотеки (кредит до 5 % на покупку производственных площадей)» [20].

Сочетание процессов обеспечения импортозамещения и последовательного перехода к полноценному технологическому суверенитету России требует также правовой регламентации указанных позиций. Термин «технологический суверенитет» изначально применялся к развитию технологии искусственного интеллекта в Российской Федерации. Под технологическим суверенитетом понималось обеспечение необходимого уровня самостоятельности Российской Федерации в области искусственного интеллекта, в том числе посредством преимущественного использования отечественных технологий искусственного интеллекта и технологических решений, разработанных на основе искусственного интеллекта [21].

В 2021 году технологический суверенитет государства был представлен, но уже в области информационно-коммуникационных технологий, как совокупность условий существования и взаимодействия государства в информационно-коммуникационной среде. Это – противодействие технологическому доминированию отдельных государств, равный доступ государств к новейшим информационно-коммуникационным технологиям и предотвращение технологической зависимости; стабильное функционирование сети «Интернет», развитие национальных информационных инфраструктур [22]. Предотвращение технологической зависимости ставится фактически во главу угла в обеспечении международной информационной безопасности.

Технологический суверенитет представляет собой высокий уровень независимости государства от импортных технологий, заменяющих либо низкого качества национальные технологии и технологическую продукцию, либо их отсутствие. В связи с чем импортозамещение как направление промышленного производства неразрывно связано с технологическим суверенитетом государства как политического явления, характеристики научно-технологической политики России.

Отметим деятельность университетов в укреплении технологического суверенитета России. Создание научно-технологической экосреды университетских кампусов выступает в настоящее время залогом развития суверенной технологической самостоятельности России. Меры государственного обеспечения научно-технологического развития, касающиеся модернизации кадрового потенциала, направлены на создание конкурентоспособных научно-исследовательских коллективов, эффективной системы воспитания и поддержки молодежи путем привлечения в науку, включая работу в Российской Федерации ученых мирового класса и молодых талантливых исследователей. Подобные меры трансформировались через федеральный национальный проект «Наука», который был разработан для ускорения научно-технологического развития Российской Федерации. В настоящее время во всех официальных документах, относящихся к определению промежуточных итогов выполнения национального проекта в области науки, последний именуется как национальный проект «Наука и университеты». Обновление названия связано отчасти с реализацией новой программы стратегического академического лидерства «Приоритет-2030» и фрагментарной неэффективностью исполнения в 2018-2019 годах национального проекта «Наука» [23]. Это было обусловлено также слабой согласованностью национального проекта «Наука» с положениями документов стратегического планирования федерального уровня. Причем, и второй этап реализации Стратегии научно-технологического развития Российской Федерации как основополагающего документа стратегического планирования возложен на Министерство науки и высшего образования Российской Федерации. Как уже отмечалось выше, выполнение Стратегии научно-технологического развития Российской Федерации предполагалось в два этапа. Правовое сопровождение первого этапа с 2017 по 2019 годы обеспечивалось Распоряжением Правительства РФ от 24 июня 2017 г. № 1325-р «План мероприятий по реализации Стратегии научно-технологического развития Российской Федерации на 2017–2019 годы (первый этап)» [24]. Согласно п. 40 Указа Президента Российской Федерации от 1 декабря 2016 г. № 642 Минобрнауки России с 2019 года будет осуществлять разработку и исполнение плана мероприятий по реализации Стратегии научно-технологического развития Российской Федерации на 2020-2025 годы (второй этап).

Заключение. В Российской Федерации сформировалась система законодательства в области научно-технологического развития, касающегося университетской экосреды параллельно с документами о стратегическом планировании и управлении. Перманентно она претерпевает систематические изменения. В регулировании научно-технологического развития органами публичной власти применяются различные методы управленческой деятельности, характеризующиеся

коллораационным подходом. Данный подход формирует мультидисциплинарные методы, использующие в своей основе экономические, социологические, статистические, правовые методы. В последнее время в большей степени используются косвенные методы государственного регулирования в области научно-технологического развития, обладающие экономическим характером (предоставление субсидий, грантов) [25].

Относительно роли университетов необходимо указать на первоочередное решение задачи формирования не просто научно-технологических университетских кампусов, а создания научно-технологической экосреды университетов и их консорциумов. Подобная экосреда обеспечит создание ими новых технологий, коммерциализации различных технологий на базе университетских кампусов и их дальнейшего продвижения в рамках производства продукции в цикле промышленных консорциумов предприятий реального сектора экономики и университетов.

Отметим, что формирование этой междисциплинарной университетской среды происходит. Прежде всего, это реализация проектов Научно-технологической инициативы и Минобрнауки: Архипелаг 2121, Архипелаг 2022, Архипелаг 2023; участие в междисциплинарных хакатонах, в кружковом движении НТИ и других научно-технологических мероприятиях, проводимых различными институтами развития, самими регионами. Государство привлекает колоссальные силы и средства для решения поставленных задач. РТУ МИРЭА в лице его акселератора также способствует развитию гармоничной среды технологического университетского кампуса.

Конечно, полному и устойчивому технологическому суверенитету России необходима выверенная система коммерциализации университетских технологий и продуктов, создание устойчивых промышленных консорциумов по производству подобной продукции, формирование прочной логистики и устойчивого цикла производства продукта на территории России. Нужна объективная оценка эффективности технологических разработок и прочного финансирования тех технологий, которые не только обеспечат импортозамещение, но и позволят занять весомую часть мирового рынка продукции. А для этого нужно развивать и экспорт образования и науки, несмотря на сложившуюся политико-социальную ситуацию.

Стоит отметить тенденцию экспансии англоязычных программ магистратуры и бакалавриата и увеличение их количества в Китае и странах Азии. Особенно это прослеживается в таких науках как медицина, педагогика и прикладные науки. Китай усиливает вступительные кампании по привлечению на обучение студентов из африканских стран, пытаясь таким образом занять глобальную часть международного рынка образования. В России же согласно данным анкетирования, большая часть респондентов не задействована в экспортных программах вузов, и, по сути, рынок экспорта образования достаточно однообразный. Следовательно, университеты-драйверы, которые будут реализовывать государственную программу «Приоритет-2030» в качестве условия участия в проекте и его исполнения, должны разрабатывать и внедрять более активно новые формы экспорта образования, выходить на дружественный международный рынок образовательных услуг. Формировать устойчивый интерес у потребителей на международном рынке к образовательным программам не столько на английском, сколько на русском языке.

Список литературы

1. Как вводили ограничительные меры в 2014 году. Досье [Электронный ресурс]. URL: https://tass.ru/info/1367443?utm_source=nova.rambler.ru&utm_medium=referral&utm_campaign=nova.rambler.ru&utm_referrer=nova.rambler.ru
2. Информация Минфина России от 30.09.2021: Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2022 год и на плановый период 2023 и 2024 годов [Электронный ресурс]. URL: <https://internet.garant.ru/#/document/402868565/paragraph/75/doclist/814/>
3. Импортзамещение как новая реальность [Электронный ресурс]. URL: https://finance.rambler.ru/other/44612397-importozameschenie-kak-novaya-realnost/?utm_source=copysharing&utm_medium=social
4. Блохин К. А. Политика импортзамещения в условиях глобализации мировой экономики / К. А. Блохин, Т. В. Шурухина // Феномен рыночного хозяйства: от истоков до наших дней. Бизнес, инновации, информационные технологии, моделирование: материалы VII Международной научно-практической конференции по экономике, посвященной памяти известного ученого и крупного организатора экономической науки на Юге России доктора экономических наук, профессора А. Ф. Сидорова, Сочи, 27–31 марта 2019 года / под ред. В. А. Сидорова и Я. С. Ядгарова / Сочи: ООО «Электронные издательские технологии», 2019. С. 131–138.
5. Козлова О. А. О необходимости перехода от политики импортзамещения к стимулированию экспорта в российской экономике (на примере текстильной промышленности) / О. А. Козлова // Известия высших учебных заведений. Технология текстильной промышленности. 2020. № 1(385). С. 88-93.
6. Абуталипова Ю. А. Инновационные направления импортзамещения в отраслях экономики / Ю. А. Абуталипова, А. И. Шинкевич // Вестник Белгородского университета кооперации, экономики и права. 2020. № 2 (81). С. 177-188.
7. Об утверждении государственной программы Российской Федерации «Развитие промышленности и повышение ее конкурентоспособности»: Постановление Правительства РФ от 15.04.2014 № 328 // Собрание законодательства РФ. 2014. № 18 (часть IV). Ст. 2173.
8. О промышленных кластерах и специализированных организациях промышленных кластеров: Постановление Правительства РФ от 31.07.2015 № 779 // Собрание законодательства РФ. 2015. № 32. Ст. 4768.
9. Об утверждении Правил предоставления из федерального бюджета субсидий участникам промышленных кластеров на возмещение части затрат при реализации совместных проектов по производству промышленной продукции кластера в целях импортзамещения: Постановление Правительства РФ от 28.01.2016 № 41 // Собрание законодательства РФ. 2016. № 6. Ст. 837.
10. Перечень-список промышленных кластеров России – 2020 год [Электронный ресурс]. URL: <https://russiaindustrialpark.ru/article/perechen-spisok-promyshlennyh-klasterov-ros-sii-2020-god>

11. Об индустриальных (промышленных) парках и управляющих компаниях индустриальных (промышленных) парков: Постановление Правительства РФ от 04.08.2015 // Собрание законодательства РФ. 2015. № 33. Ст. 4827.

12. Об утверждении требований к реализации мероприятий, осуществляемых субъектами Российской Федерации, бюджетам которых предоставляются субсидии на государственную поддержку малого и среднего предпринимательства, а также физических лиц, применяющих специальный налоговый режим «Налог на профессиональный доход», в субъектах Российской Федерации, направленных на достижение целей, показателей и результатов региональных проектов, обеспечивающих достижение целей, показателей и результатов федеральных проектов, входящих в состав национального проекта «Малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы», и требований к организациям, образующим инфраструктуру поддержки субъектов малого и среднего предпринимательства: Приказ Министерства экономического развития РФ от 26.03.2021 № 142 [Электронный ресурс]. Официальный интернет-портал правовой информации от 21.05.2021 № 0001202105210015. URL: www.pravo.gov.ru

13. О промышленных технопарках и управляющих компаниях промышленных технопарков: Постановления Правительства РФ от 27.12.2019 № 1863 // Собрание законодательства РФ. 2020. № 2 (часть I). Ст. 164.

14. Об утверждении Методических рекомендаций по подготовке заявки на возмещение затрат на создание, модернизацию и (или) реконструкцию объектов инфраструктуры индустриального парка или промышленного технопарка: Приказ Министерства промышленности и торговли РФ от 27.01.2017 № 211 [Электронный ресурс]. URL: <https://internet.garant.ru/#/document/71631898/paragraph/26/doclist/1197/>

15. О внесении изменений в постановление Правительства Российской Федерации от 27.12.2019 № 1863 и признании утратившим силу отдельного положения акта Правительства Российской Федерации: Постановление Правительства РФ от 04.07.2022 № 1202 // Собрание законодательства РФ. 2022. № 28. Ст. 5117.

16. Об утверждении Перечня требований к объектам технологической инфраструктуры промышленных технопарков: Приказ Министерства промышленности и торговли РФ от 23.09.2020 № 3221 [Электронный ресурс]. Официальный интернет-портал правовой информации от 23.10.2020 № 0001202010230011. URL: www.pravo.gov.ru

17. О внесении изменений в требования к реализации мероприятий, осуществляемых субъектами Российской Федерации, бюджетам которых предоставляются субсидии на государственную поддержку малого и среднего предпринимательства, а также физических лиц, применяющих специальный налоговый режим «Налог на профессиональный доход», в субъектах Российской Федерации, направленных на достижение целей, показателей и результатов региональных проектов, обеспечивающих достижение целей, показателей и результатов федеральных проектов, входящих в состав национального проекта «Малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы», и требования к организациям, образующим инфраструктуру поддержки субъектов малого и среднего предпринимательства: Приказ Министерства экономического развития

РФ от 24.03.2022 № 149 [Электронный ресурс]. URL: Официальный интернет-портал правовой информации (www.pravo.gov.ru) от 01.04.2022 № 0001202204010043.

18. Перечень-список технопарков России – 2022 год [Электронный ресурс]. URL: https://russiaindustrialpark.ru/tehnopark_catalog_perecheny_spisok_russia

19. Владимир Путин представил план прорыва [Электронный ресурс]. URL: <https://www.kommersant.ru/doc/5421339>

20. Владимир Путин представил план прорыва [Электронный ресурс]. URL: <https://www.kommersant.ru/doc/5421339>

21. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10.10.2019 № 490 // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

22. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности: Указ Президента РФ от 12.04.2021 № 213 // Собрание законодательства РФ. 2021. № 16 (часть I). Ст. 2746.

23. Отчет о промежуточных результатах экспертно-аналитического мероприятия «Мониторинг хода реализации мероприятий национального проекта «Наука», необходимых для выполнения задач, поставленных в Указе Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Бюллетень Счетной палаты Российской Федерации. Специальный выпуск «Реализация национальных проектов». 2020. № 265. С. 122–171.

24. Собрание законодательства РФ. 2017. № 28. Ст. 4174; 2017. № 41. Ст. 5992.

25. О мерах по реализации программы стратегического академического лидерства «Приоритет-2030»: Постановление Правительства РФ от 13.05.2021 № 729.

СОДЕРЖАНИЕ | CONTENTS

МУЛЬТИДИСЦИПЛИНАРНЫЕ АСПЕКТЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ |
MULTIDISCIPLINARY ASPECTS OF DIGITAL TRANSFORMATION

<i>Айларова З. А.</i> ВЛИЯНИЕ ЦИФРОВОГО СЛЕДА НА ПОВСЕДНЕВНУЮ И ПРОФЕССИОНАЛЬНУЮ ДЕЯТЕЛЬНОСТЬ <i>Ailarova Z.</i> THE IMPACT OF THE DIGITAL FOOTPRINT ON EVERYDAY AND PROFESSIONAL ACTIVITIES	6
<i>Алексеев Н. В.</i> КОНЦЕПЦИЯ ТВОРЧЕСКОГО СТИЛЯ В ЭПОХУ НЕЙРОСЕТЕВОГО ИСКУССТВА <i>Alekseev N.</i> THE CONCEPT OF CREATIVE STYLE IN THE AGE OF NEURAL NETWORK ART	11
<i>Алешина А. В., Булгаков А. Л.</i> ФИНАНСОВОЕ МОШЕННИЧЕСТВО И ЦИФРОВЫЕ ТЕХНОЛОГИИ <i>Aleshina A., Bulgakov A.</i> FINANCIAL FRAUD AND DIGITAL TECHNOLOGIES.....	17
<i>Анурова М. В.</i> БЛОКЧЕЙН КАК ИЗБИРАТЕЛЬНАЯ ТЕХНОЛОГИЯ: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ <i>Anurova M.</i> BLOCKCHAIN AS A SELECTIVE TECHNOLOGY: ADVANTAGES AND DISADVANTAGES.....	28
<i>Аракелян А. А.</i> МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ: ВИКТИМОЛОГИЧЕСКАЯ ПРОФИЛАКТИКА <i>Arakelyan A.</i> FRAUD ON THE INTERNET: VICTIMOLOGICAL PREVENTION	32
<i>Арланова А. А.</i> ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ СИСТЕМЫ ТУРКМЕНИСТАНА <i>Arlanova A.</i> PRIORITY AREAS OF DIGITAL TRANSFORMATION OF THE FINANCIAL AND ECONOMIC SYSTEM OF TURKMENISTAN	34
<i>Арланова А. А., Чарыев М., Дурдыев О.</i> ИННОВАЦИОННЫЕ РЕФОРМЫ ЦИФРОВИЗАЦИИ ЭНЕРГЕТИЧЕСКОГО СЕКТОРА ТУРКМЕНИСТАНА <i>Arlanova A., Charyev M., Durdyev O.</i> INNOVATIVE REFORMS OF DIGITALIZATION OF THE ENERGY SECTOR OF TURKMENISTAN	39
<i>Артамонов А. Н.</i> ИЗМЕНЕНИЕ ТРАДИЦИОННЫХ СПОСОБОВ КОММУНИКАЦИИ КАК БЛАГО И ТРАДИЦИОННЫХ ЦЕННОСТЕЙ КАК ПУТЬ В БЕЗДНУ <i>Artamonov A.</i> CHANGING TRADITIONAL WAYS OF COMMUNICATION AS A BLESSING AND TRADITIONAL VALUES AS A PATH TO THE ABYSS.....	42

<i>Архангельская М. А.</i> ИСПОЛЬЗОВАНИЕ 3D-ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ СУДЕБНО-МЕДИЦИНСКОГО ЭКСПЕРТА <i>Arhangel'skaya M.</i> THE USE OF 3D TECHNOLOGIES IN THE ACTIVITIES OF A FORENSIC MEDICAL EXPERT.....	48
<i>Бабаназаров Н. Ш.</i> ТРУДОВЫЕ ОТНОШЕНИЯ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ <i>Babanazarov N.</i> LABOR RELATIONS IN THE CONTEXT OF DIGITAL TRANSFORMATION	52
<i>Балахонцев Г. М.</i> ИНФОРМАТИЗАЦИЯ ВНУТРЕННЕГО ФИНАНСОВОГО КОНТРОЛЯ <i>Balahoncev G.</i> INFORMATIZATION OF THE INTERNAL FINANCIAL CONTROL	55
<i>Бурангулов Э. Р.</i> ЦИФРОВЫЕ ТЕХНОЛОГИИ В ВЫСШЕМ ОБРАЗОВАНИИ РОССИИ: ПРОБЛЕМЫ В СФЕРЕ ИНТЕЛЛЕКТУАЛЬНОГО ПРАВА <i>Burangulov E.</i> DIGITAL TECHNOLOGIES IN HIGHER EDUCATION IN RUSSIA: PROBLEMS IN THE FIELD OF INTELLECTUAL PROPERTY LAW	61
<i>Вебер Д. С., Гадельшина С. Р.</i> ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ CRM-СИСТЕМЫ <i>Veber D., Gadelshina S.</i> PROTECTION OF CONFIDENTIAL INFORMATION WHEN USING THE SYSTEM	64
<i>Вербицкая Т. В.</i> ЦИФРОВЫЕ КОПИИ ПРАВОВЫХ АКТОВ XVIII–XX ВЕКОВ ДЛЯ ИЗУЧЕНИЯ ИСТОРИИ ПРАВА (НА ПРИМЕРЕ ОПЫТА СОЗДАНИЯ И ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОГО ПОРТАЛА О ПРОМЫШЛЕННИКАХ ДЕМИДОВЫХ) <i>Verbickaya T.</i> DIGITAL COPIES OF LEGAL ACTS OF THE XVIII–XX CENTURIES FOR THE STUDY OF THE HISTORY OF LAW (ON THE EXAMPLE OF THE EXPERIENCE OF CREATING AND FUNCTIONING OF THE INFORMATION PORTAL ABOUT INDUSTRIALISTS DEMIDOV)	67
<i>Воверко Ю. Е., Шаповал А. С.</i> ПРЕПЯТСТВИЯ ПРИ ПОДПИСАНИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСЬЮ ДОКУМЕНТОВ ПРИ ЗАКЛЮЧЕНИИ МЕЖДУНАРОДНЫХ СДЕЛОК <i>Voverko Yu., Shapoval A.</i> OBSTACLES ARISING WHEN SIGNING DOCUMENTS BY ELECTRONIC DIGITAL SIGNATURE WHEN CONCLUDING INTERNATIONAL TRANSACTIONS.....	74
<i>Волкова Г. Е.</i> ТРАНСФОРМАЦИЯ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА <i>Volkova G.</i> TRANSFORMATION OF THE RIGHT TO PRIVACY IN THE CONDITIONS OF DIGITALIZATION OF SOCIETY.....	78

<i>Габович А. А.</i> ФОРМИРОВАНИЕ ГРАЖДАНСКОЙ ПОЗИЦИИ СТУДЕНТОВ – БУДУЩИХ ЮРИСТОВ В КОНТЕКСТЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ <i>Gabovich A.</i> FORMATION OF CIVIC POSITION STUDENTS – FUTURE LAWYERS IN THE CONTEXT OF DIGITAL TRANSFORMATION.....	83
<i>Гадельшина С. Р., Вебер Д. С.</i> ЧАТ-БОТЫ КАК ИНСТРУМЕНТАРИЙ СОВРЕМЕННОГО ЮРИСТА <i>Gadelshina S., Veber D.</i> CHATBOTS AS A TOOLKIT FOR THE MODERN LAWYER	85
<i>Галкин Н. А.</i> ВЛИЯНИЕ «ИНТЕРНЕТА ВСЕГО» НА ПРАВО <i>Galkin N.</i> THE IMPACT OF THE INTERNET OF EVERYTHING ON THE LAW	89
<i>Гамбеева Ю. Н., Кожухова Н. Н.</i> РАЗВИТИЕ ИНСТИТУТА САМОЗАНЯТОСТИ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ПЛАТФОРМ <i>Gambееva Yu., Kozhuhova N.</i> DEVELOPMENT OF THE INSTITUTION OF SELF-EMPLOYMENT USING DIGITAL PLATFORMS	92
<i>Генюш В. В.</i> ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ВОПРОСЫ ЦИФРОВИЗАЦИИ ДОКУМЕНТООБОРОТА В ЮРИДИЧЕСКОЙ КЛИНИКЕ <i>Genyush V.</i> ORGANIZATIONAL AND LEGAL ISSUES OF DIGITALIZATION OF DOCUMENT FLOW IN A LAW CLINIC.....	101
<i>Глянц Е. М.</i> ПРОТИВОДЕЙСТВИЕ КИБЕРМОШЕННИЧЕСТВУ: ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ <i>Glyanc E.</i> COUNTERING CYBERFRAUD: PROBLEMS OF THEORY AND PRACTICE.....	108
<i>Гокунь Ю. С.</i> СОЗДАНИЕ ЕДИНОГО РЕГИСТРА СУРРОГАТНЫХ МАТЕРЕЙ И ДОНОРОВ БИОМАТЕРИАЛОВ И ОБЕСПЕЧЕНИЕ ЕГО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ <i>Gokun Yu.</i> CREATION OF A UNIFIED REGISTER OF SURROGATE MOTHERS AND DONORS OF BIOMATERIALS AND ENSURING ITS INFORMATION SECURITY.....	116
<i>Горячев И. В.</i> О ЦИФРОВЫХ ТЕХНОЛОГИЯХ УПРАВЛЕНИЯ КАДРОВЫМ СОСТАВОМ ГОСУДАРСТВЕННОЙ СЛУЖБЫ В СОВРЕМЕННЫХ ИССЛЕДОВАНИЯХ <i>Goryachev I.</i> ABOUT DIGITAL TECHNOLOGIES FOR MANAGING THE STAFF OF THE PUBLIC SERVICE IN MODERN RESEARCH	122
<i>Гретченко А. И., Гретченко А. А.</i> ОЦЕНКА УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ТРУДОВЫХ ПРОЦЕССОВ <i>Gretchenko A., Gretchenko A.</i> INDUSTRY 4.0 AND ASSESSMENT OF THE LEVEL OF INFORMATION SECURITY IN RUSSIA IN THE CONTEXT OF DIGITALIZATION OF LABOR PROCESSES.....	126

<i>Евсеева С. Д.</i> КОНЦЕПЦИЯ «УМНЫЙ ГОРОД» В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ <i>Evseeva S.</i> THE CONCEPT OF “SMART CITY” IN THE CONTEXT OF THE DIGITAL TRANSFORMATION OF THE RUSSIAN FEDERATION.....	140
<i>Еремеева А. В.</i> ЦИФРОВИЗАЦИЯ В СФЕРЕ ГОСУДАРСТВЕННЫХ ЗАКУПОК: ПРЕТЕНЗИОННАЯ РАБОТА КАК ЧАСТЬ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА <i>Eremeeva A.</i> DIGITALIZATION IN THE FIELD OF PUBLIC PROCUREMENT: CLAIM WORK AS PART OF ELECTRONIC DOCUMENT MANAGEMENT.....	148
<i>Есиркепова М. М.</i> ДИСТАНЦИОННАЯ РАБОТА В УСЛОВИЯХ ПАНДЕМИИ КОРОНАВИРУСНОЙ ИНФЕКЦИИ <i>Esirkepova M.</i> REMOTE WORK IN CONDITIONS OF CORONAVIRUS INFECTION.....	153
<i>Зайцева И. А.</i> ИННОВАЦИОННЫЕ ВОЗМОЖНОСТИ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ФОРМИРОВАНИИ ДОСТУПНОЙ СРЕДЫ ДЛЯ ИНВАЛИДОВ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ В СОВРЕМЕННОМ ОБЩЕСТВЕ <i>Zaiceva I.</i> DIGITAL INNOVATION IN CREATING AN ACCESSIBLE ENVIRONMENT FOR PEOPLE WITH DISABILITIES: CHALLENGES AND SOLUTIONS IN TODAY’S SOCIETY.....	158
<i>Захарова Д. О.</i> ПРОБЛЕМЫ ВЕРИФИКАЦИИ С ТОЧКИ ЗРЕНИЯ ЗАКОНА И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ <i>Zaharova D.</i> VERIFICATION PROBLEMS FROM THE POINT OF VIEW OF THE LAW AND INFORMATION SECURITY	163
<i>Зыкова В. В.</i> МЕЖДУНАРОДНАЯ ВАЛЮТА ДЛЯ РАСЧЕТОВ МЕЖДУ ГОСУДАРСТВАМИ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА <i>Zykova V.</i> INTERNATIONAL CURRENCY FOR SETTLEMENTS BETWEEN THE SHANGHAI COOPERATION ORGANISATION	166
<i>Ибатуллина Л. Р.</i> ПРЕДУПРЕЖДЕНИЕ ПРИМЕНЕНИЯ ДОПИНГА, СУБСТАНЦИЙ И МЕТОДОВ, ЗАПРЕЩЕННЫХ ДЛЯ ИСПОЛЬЗОВАНИЯ В СПОРТЕ, С ПОМОЩЬЮ ЦИФРОВЫХ ТЕХНОЛОГИЙ <i>Ibatullina L.</i> PREVENTION OF THE USE OF DOPING, SUBSTANCES AND METHODS PROHIBITED FOR USE IN SPORTS USING DIGITAL TECHNOLOGIES	169
<i>Ильина О. П.</i> АРХИТЕКТУРА ПРЕДПРИЯТИЯ КАК ИНСТРУМЕНТ РЕГУЛИРОВАНИЯ ПРОЕКТА ЦИФРОВОЙ ТРАНСФОРМАЦИИ <i>Ilina O.</i> THE ENTERPRISE ARCHITECTURE AS A TOOL FOR LEGAL REGULATION OF THE DIGITAL TRANSFORMATION PROJECT	171

<i>Касенова Г. Т., Смаилова М. Т.</i> ВОЗМОЖНОСТИ ПРОЦЕССА ЦИФРОВИЗАЦИИ В СФЕРЕ ОБРАЗОВАНИЯ В КАЗАХСТАНЕ <i>Kasenova G., Smailova M.</i> POSSIBILITIES OF THE DIGITAL PROCESS IN EDUCATION IN KAZAKHSTAN.....	177
<i>Курсанова О. Г.</i> ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ <i>Kirsanova O.</i> LEGAL ASPECTS OF PERSONAL DATA PROTECTION IN THE CONTEXT OF DIGITALIZATION	187
<i>Комлев Е. Ю.</i> ЗАСЕДАНИЯ ПРЕДСТАВИТЕЛЬНЫХ ОРГАНОВ МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЙ В ДИСТАНЦИОННОМ ФОРМАТЕ: ПРАКТИКА И ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ <i>Komlev E.</i> LOCAL COUNCIL SESSIONS IN REMOTE FORMAT: PRACTICE AND PROSPECTS OF LEGAL REGULATION	196
<i>Костылева Е. Д.</i> СОЦИАЛЬНЫЕ ГАРАНТИИ РЕАЛИЗАЦИИ ПРАВА НА ОБРАЗОВАНИЕ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ <i>Kostyleva E.</i> SOCIAL GUARANTEES FOR THE REALIZATION OF THE RIGHT TO EDUCATION IN THE DIGITAL AGE.....	200
<i>Котилевец И. Д.</i> ДЕКОМПОЗИЦИОННЫЙ ПОДХОД В ОПРЕДЕЛЕНИИ ТЕМАТИКИ И МЕХАНИЗМА ПРОЕКТНО-ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫПОЛНЕНИИ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ <i>Kotilevec I.</i> DECOMPOSITIONAL APPROACH IN DETERMINING THE SUBJECT AND MECHANISM OF DESIGN AND RESEARCH ACTIVITIES WHEN PERFORMING FINAL QUALIFICATION WORKS	205
<i>Кудинов В. В.</i> ПОТЕНЦИАЛ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА С ПРИМЕНЕНИЕМ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ В ОБРАЗОВАНИИ <i>Kudinov V.</i> THE POTENTIAL OF USING ARTIFICIAL INTELLIGENCE USING METHODS OF INTELLIGENT DATA ANALYSIS IN EDUCATION	211
<i>Мальцев И. В.</i> ГОСУДАРСТВЕННЫЕ СИМВОЛЫ В СОДЕРЖАНИИ ЭЛЕКТРОННОЙ ПОДПИСИ <i>Malcev I.</i> STATE SYMBOLS IN THE CONTENT OF ELECTRONIC SIGNATURE	224
<i>Мезенцева А. И.</i> ПАТЕНТ КАК СРЕДСТВО ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ ИТ-РАЗРАБОТОК В СФЕРЕ ТЕХНИЧЕСКОГО ОБРАЗОВАНИЯ <i>Mezenceva A.</i> PATENT AS A MEANS OF IT DEVELOPMENTS PROTECTING INTELLECTUAL PROPERTY IN THE TECHNICAL EDUCATION FIELD	230

<i>Мистров Л. Е.</i> МЕТОД ЦИФРОВЫХ ТЕХНОЛОГИЙ ДЛЯ МОДЕЛИРОВАНИЯ ЗАДАЧИ СИНТЕЗА СУДЕБНЫХ РЕШЕНИЙ ПО РАЗРЕШЕНИЮ КОНФЛИКТОВ <i>Mistrov L.</i> DIGITAL TECHNOLOGY METHOD FOR SIMULATION OF THE PROBLEM OF SYNTHESIS OF JUDICIAL DECISIONS ON CONFLICT RESOLUTION	234
<i>Мямиев А. Х., Пердяев К.</i> КОММЕРЧЕСКИЕ УГРОЗЫ В ТОРГОВОЙ СИСТЕМЕ <i>Myamiev A., Perdyayev K.</i> COMMERCIAL THREATS IN THE TRADING SYSTEM.....	247
<i>Нижник Л. С.</i> ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПУБЛИЧНО-ПРАВОВЫХ ОТНОШЕНИЙ В СФЕРЕ ЭКОЛОГИИ <i>Nizhnik L.</i> DIGITAL TRANSFORMATION OF PUBLIC LEGAL RELATIONS IN THE FIELD OF ECOLOGY	249
<i>Нобатов А. М., Маткаримов А. И.</i> ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ В ЗАЩИТЕ КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ЭКСПЛОЙТОВ <i>Nobatov A., Matkarimov A.</i> PRIORITY AREAS IN PROTECTION OF COMPUTER SYSTEMS AND AGAINST EXPLOITS	254
<i>Оразов Б. К.</i> ОСОБЕННОСТИ РАЗВИТИЯ ЧЕЛОВЕЧЕСКОГО КАПИТАЛА В ЦИФРОВОЙ ЭКОНОМИКЕ <i>Orazov B.</i> FEATURES OF THE DEVELOPMENT OF HUMAN CAPITAL IN THE DIGITAL ECONOMY	257
<i>Петров А. А.</i> ВОСПРОИЗВОДСТВО ОТЕЧЕСТВЕННОЙ ИТ-ИНДУСТРИИ В УСЛОВИЯХ САНКЦИЙ <i>Petrov A.</i> REPRODUCTION OF THE DOMESTIC IT-INDUSTRY IN THE CONDITIONS OF SANCTIONS.....	260
<i>Пискунов Д. А., Лесникова П. С.</i> КОНКУРЕНЦИЯ В СФЕРЕ 5G-ТЕХНОЛОГИЙ И МЕСТО РОССИИ <i>Piskunov D., Lesnikova P.</i> 5G-COMPETITION AND RUSSIA'S PLACE IN IT.....	272
<i>Прибытко А. А.</i> ПРАКТИКА ИНВЕСТИЦИЙ В РЕСПУБЛИКЕ БЕЛАРУСЬ В РАМКАХ ПАРКА ВЫСОКИХ ТЕХНОЛОГИЙ <i>Pribytko A.</i> THE PRACTICE OF INVESTMENTS IN THE REPUBLIC OF BELARUS ON THE EXAMPLE OF A HIGH-TECH PARK	284
<i>Сабирова В. К., Абытова Г. З., Умарова А. А., Айзирек А.</i> СМИ ЮЖНОГО РЕГИОНА НА РУССКОМ И КЫРГЫЗСКОМ ЯЗЫКАХ И ИХ РОЛЬ В ВОСПИТАНИИ МОЛОДЕЖИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ <i>Sabirova V., Abytova G., Umarova A., Aizirek A.</i> THE MASS MEDIA OF THE SOUTHERN REGION IN RUSSIAN AND KYRGYZ LANGUAGES AND THEIR ROLE IN EDUCATING YOUNG PEOPLE IN THE CONDITIONS OF DIGITALIZATION	289

<i>Сабодах И. В., Давыдова Д. А.</i> ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ДЛЯ РАССЛЕДОВАНИЯ ИСКАЖЕНИЯ ФИНАНСОВЫХ ПОКАЗАТЕЛЕЙ КОМПАНИИ <i>Sabodah I., Davydova D.</i> USING DIGITAL TECHNOLOGY TO INVESTIGATE THE COMPANY'S FINANCIAL MISSTATEMENTS	294
<i>Савлаев Д. В.</i> ЦИФРОВЫЕ ТЕХНОЛОГИИ КАК МЕХАНИЗМ ПОВЫШЕНИЯ ОБЪЕМОВ ЭКСПОРТА РОССИЙСКИХ ТОВАРОВ <i>Savlaev D.</i> DIGITAL TECHNOLOGIES AS A MECHANISM TO INCREASE EXPORTS OF RUSSIAN GOODS	298
<i>Семенухин А. Л.</i> ПРОБЛЕМЫ НАЛОГООБЛОЖЕНИЯ ЦИФРОВЫХ АКТИВОВ <i>Sezenihin A.</i> PROBLEMS OF TAXATION OF DIGITAL ASSETS	302
<i>Соломин С. К.</i> К ВОПРОСУ О ПРАВОВОЙ КВАЛИФИКАЦИИ КЕШБЭКА ПО БАНКОВСКОЙ КАРТЕ <i>Solomin S.</i> TO THE QUESTION OF LEGAL QUALIFICATION OF CASHBACK ON BANK CARD	309
<i>Соляник С. В., Соляник В. В.</i> ЦИФРОВИЗАЦИЯ ЗООТЕХНИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ КАК МЕХАНИЗМ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЖИВОТНОВОДСТВА НОРМАМИ АГРАРНОГО ПРАВА <i>Solyanik S., Solyanik V.</i> DIGITALIZATION OF ZOOTECHNICAL ACTIVITIES AS A MECHANISM OF LEGAL REGULATION OF ANIMAL HUSBANDRY BY NORMS OF AGRARIAN LAW	314
<i>Сомонов В. В., Николаев А. С.</i> ИСПОЛЬЗОВАНИЕ ПАТЕНТНОЙ АНАЛИТИКИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИННОВАЦИОННЫХ ПРОЕКТОВ <i>Somonov V., Nikolaev A.</i> THE INFLUENCE OF PATENT ANALYTICS ON THE INFORMATION SECURITY OF INNOVATIVE PROJECTS	324
<i>Спешилова Н. В., Мамедов А. А.</i> ВЫГОДЫ, РИСКИ, ПРОБЛЕМЫ И МАСШТАБЫ ЦИФРОВИЗАЦИИ <i>Speshilova N., Mamedov A.</i> BENEFITS, RISKS, PROBLEMS AND SCALE OF DIGITALIZATION	332
<i>Степаненко Д. В.</i> СРАВНИТЕЛЬНЫЙ ОБЗОР МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ИЗ МЕТОДИКИ ФСТЭК РОССИИ И МАТРИЦ MITRE ATT&CK <i>Stepanenko D.</i> COMPARATIVE REVIEW OF INFORMATION SECURITY THREAT MODELING FROM THE FSTEC METHODOLOGY AND MITRE ATT&CK MATRICES.....	337
<i>Суслов И. Д.</i> СТАТУС ОНЛАЙН-ОБУЧЕНИЯ В СОВРЕМЕННОЙ СИСТЕМЕ ОБРАЗОВАНИЯ <i>Suslov I.</i> THE STATUS OF ONLINE TEACHING IN THE MODERN EDUCATION SYSTEM.....	346

<i>Ташбаев И. О., Омонкулов Э.</i> ЦИФРОВАЯ ЭКОНОМИКА – ВАЖНЫЙ ФАКТОР РАЗВИТИЯ НОВОГО УЗБЕКИСТАНА <i>Tashbaev I., Omonkulov E.</i> DIGITAL ECONOMY, IS AN IMPORTANT FACTOR IN THE DEVELOPMENT OF THE NEW UZBEKISTAN	351
<i>Трахов А. И., Бешукова З. М.</i> ПРЕДУПРЕЖДЕНИЕ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА: РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ <i>Trahov A., Beshukova Z.</i> TELEPHONE FRAUD PREVENTION: RUSSIAN AND FOREIGN EXPERIENCE.....	357
<i>Трусов Ю. А., Антипов А. В.</i> ПРАВО НА ЗАБВЕНИЕ: ОПЫТ ПРАКТИЧЕСКОГО АНАЛИЗА <i>Trusov Yu., Antipov A.</i> RIGHT, TO BE FORGOTTEN: THE EXPERIENCE OF THE PRACTICAL ANALYSIS	362
<i>Фартушинова А.</i> ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ СРЕДЕ <i>Fartushonova A.</i> LEGAL REGULATION INFORMATION SECURITY IN THE DIGITAL ENVIRONMENT	366
<i>Федоров Р. В.</i> ТЕОРЕТИКО-ПРАВОВЫЕ АСПЕКТЫ МЕТОДА ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ТЕКСТА И ДАННЫХ <i>Fedorov R.</i> THEORETICAL AND LEGAL ASPECTS OF THE TEXT AND DATA MINING	371
<i>Харина О. А.</i> ЦИФРОВИЗАЦИЯ ПОЛИТИКИ В ИНДИИ: ОПЫТ ДЛЯ РОССИИ <i>Harina O.</i> DIGITALIZATION OF POLITICS IN INDIA: EXPERIENCE FOR RUSSIA	374
<i>Цветкова А. Д.</i> СФЕРЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ КЕЙЛОГЕРОВ В ЮРИСПРУДЕНЦИИ <i>Cvetkova A.</i> SCOPE OF APPLICATION OF KEYLOGGER TECHNOLOGY IN JURISPRUDENCE.....	381
<i>Чеджемов С. Р.</i> ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И ИНФОДЕМИЯ <i>Chedzhetov S.</i> INFORMATION PROCESSES AND INFODEMIA.....	387
<i>Честнов Е. А., Цветков К. Т.</i> ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ВЕБ-АРХИВОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С РАСПРОСТРАНЕНИЕМ НЕГАТИВНОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ <i>Chestnov E., Cvetkov K.</i> THE POSSIBILITY OF USING WEB ARCHIVES IN THE INVESTIGATIONS OF CRIMES RELATED TO THE DISTRIBUTION OF NEGATIVE CONTENT ON THE INTERNET	394

Чукреев В. А. СПОРНЫЕ ВОПРОСЫ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ
ОБОРОТА ПОРНОГРАФИЧЕСКИХ МАТЕРИАЛОВ В ВИРТУАЛЬНОМ
ПРОСТРАНСТВЕ: РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ |
Chukreev V. CONTROVERSIAL ISSUES OF CRIMINAL AND LEGAL
ASSESSMENT OF THE TURNOVER OF PORNOGRAPHIC MATERIALS
IN THE VIRTUAL INDUSTRY: RUSSIAN AND FOREIGN EXPERIENCE 400

Шевалдина Е. И. СОВЕРШЕНСТВОВАНИЕ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ
КОНТРОЛЯ ЗА БЕЗНАДЗОРНЫМИ ЖИВОТНЫМИ |
Shevaldina E. IMPROVEMENT OF THE INFORMATION AND ANALYTICAL
CONTROL SYSTEM FOR NEGLECTED ANIMALS..... 404

Якубова Г. Ф. ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ БЛОКЧЕЙН
В НЕФТЕГАЗОВОЙ ПРОМЫШЛЕННОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ |
Yakubova G. APPLICATION OF BLOCKCHAIN TECHNOLOGIES IN THE OIL
AND GAS INDUSTRY OF THE RUSSIAN FEDERATION 407

МУЛЬТИСЦИПЛИНАРНЫЙ ХАКАТОН | MULTI-DISCIPLINARY HACKATHON

Головачев К. В., Куликова О. Н. ЭФФЕКТИВНОСТЬ
ИНФОРМАЦИОННОЙ СИСТЕМЫ МЕЖВЕДОМСТВЕННОГО
ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ ГЕНЕРАЛЬНОЙ
ПРОКУРАТУРЫ В АНТИКОРРУПЦИОННОЙ ДЕЯТЕЛЬНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ |
Golovachev K., Kulikova O. THE EFFECTIVENESS OF THE
INFORMATION SYSTEM OF INTERDEPARTMENTAL
ELECTRONIC INTERACTION OF THE PROSECUTOR
GENERAL'S OFFICE IN THE ANTI-CORRUPTION ACTIVITIES
OF THE RUSSIAN FEDERATION 411

Ершова Ю. В., Лысенко В. К. КРИПТОВАЛЮТА
КАК ОБЪЕКТ КОРПОРАТИВНОГО ПРАВА: ТЕНДЕНЦИИ
РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА |
Ershova Yu., Lysenko V. CRYPTOCURRENCY AS AN OBJECT
OF CORPORATE LAW: TRENDS IN THE DEVELOPMENT
OF LEGISLATION..... 417

Карпухин М. Ю., Хомякова М. А. ПЕРСПЕКТИВЫ ЦИФРОВИЗАЦИИ
СЕЛЬСКОГО ХОЗЯЙСТВА ДО 2030 ГОДА: ПРАВОВОЙ АСПЕКТ |
Karpuhin M., Homyakova M. PROSPECTS OF DIGITALIZATION
OF AGRICULTURE UNTIL 2030: LEGAL ASPECT 422

<i>Касьянова Е. Л., Черкас М. В.</i> НАУЧНО-МЕТОДИЧЕСКИЕ ОСНОВЫ КАРТОГРАФИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРАВООЗАЩИТНОЙ ДЕЯТЕЛЬНОСТИ <i>Kasyanova E., Cherkas M.</i> SCIENTIFIC AND METHODOLOGICAL FOUNDATIONS OF CARTOGRAPHIC SUPPORT OF HUMAN RIGHTS ACTIVITIES	427
<i>Штепа И. В.</i> ЛОГИКА И МЕТОДОЛОГИЯ ЦИФРОВИЗАЦИИ НАУКИ: ПРИМЕНИМОСТЬ РАБОТ ПО СИНЕРГЕТИКЕ В СОВРЕМЕННЫХ ИССЛЕДОВАНИЯХ <i>Shtepa I.</i> LOGIC AND METHODOLOGY OF DIGITALIZATION OF SCIENCE: APPLICABILITY OF WORKS ON SYNERGETICS IN MODERN RESEARCH	444
<i>Щукина Т. В.</i> ВОПРОСЫ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА РОССИИ: ПУБЛИЧНО-ПРАВОВЫЕ АСПЕКТЫ <i>Shchukina T.</i> QUESTIONS OF TECHNOLOGICAL SOVEREIGNTY OF RUSSIA: PUBLIC LAW ASPECTS	451

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
I Международной научно-практической конференции

23 сентября 2022 г.
г. Казань

В шести томах
Том 6

*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 редакторы: *О. А. Аймурзаева, С. Р. Каримова*
Дизайн обложки: *Г. И. Загретдинова*

ISBN 978-5-8399-0773-7



Подписано в печать 27.10.2022. Формат 60×84/16.
Гарнитура PT Astra Serif, 9. Усл. печ. л. 27,44. Уч.-изд. л. 32,92.
Тираж 2000 экз. Заказ № 112.



Издательство «Познание» Казанского инновационного университета им. В. Г. Тимирязова
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



ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ



JOURNAL OF DIGITAL
TECHNOLOGIES AND LAW

ХАЙТЕК

it.world

technoverly

International Journal of
Law in Changing World

РАПСИ Российское агентство
правовой и судебной информации

