



Как цитировать: Цифровые технологии и право: сборник научных трудов III Международной научно-практической конференции (г. Казань, 20 сентября 2024 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2024. EDN: QONPHL. http://dx.doi.org/10.21202/978-5-8399-0843-7_3 – 1 CD-ROM. – Загл. с титул. экрана. – Текст: электронный.

For citation: Digital Technologies and Law: collection of scientific papers of the III International Scientific and Practical Conference (Kazan, 2024, September 20) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 3. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2024. EDN: QONPHL. http://dx.doi.org/10.21202/978-5-8399-0843-7_3 – 1 CD-ROM. – Title from the title screen. – Text: electronic.



ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
III Международной научно-практической конференции

20 сентября 2024 г.

г. Казань

В шести томах

Том 3



DIGITAL TECHNOLOGIES AND LAW

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

2023, September 22

Kazan

In 6 volumes

Volume 3

УДК 004:34(063)
ББК 67с51я43
Ц75

Издается по решению редакционно-издательского совета
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»;

К. А. Пономарева, доктор юридических наук, доцент, ведущий научный сотрудник Центра налоговой политики Научно-исследовательского финансового института Министерства финансов Российской Федерации, профессор кафедры правового обеспечения рыночной экономики Высшей школы правоведения Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации;

Е. А. Русскевич, доктор юридических наук, доцент, профессор кафедры уголовного права Московского государственного юридического университета имени О. Е. Кутафина;

К. Л. Томашевский, доктор юридических наук, профессор, заместитель декана юридического факультета по научной работе, профессор кафедры гражданского и предпринимательского права Казанского инновационного университета имени В. Г. Тимирязова;

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 III Международной научно-практической конференции (г. Казань, 20 сентября 2024 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2024. EDN: QONPHL. http://dx.doi.org/10.21202/978-5-8399-0843-7_3 – 1 CD-ROM. – Загл. с титул. экрана. – Текст: электронный.

Системные требования: операционные системы Linux, Windows; 120 Мб; 16 Мб; PDF Reader; дисковод CD-ROM, мышь

ISBN 978-5-8399-0859-8

ISBN 978-5-8399-0843-7 (Том 3)

Вошедшие в сборник научные труды приурочены к III Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 20 сентября 2024 г. в Казани в рамках Международного форума Kazan Digital Week 2024, организуемого Правительством Российской Федерации совместно с Кабинетом Министров Республики Татарстан.

На конференции обсуждался широкий спектр теоретико-методологических, практико-ориентированных, междисциплинарных и отраслевых вопросов, касающихся приоритетов развития правового регулирования цифровых технологий, нормативного контроля над цифровой средой, перспектив влияния права на формирование и развитие новых общественных отношений.

Научные труды представлены тома систематизированы по современным трендам развития цифровых технологий в системе уголовно-правовых отношений; отдельно в формате мультидисциплинарного «хакатона» обобщены взгляды и подходы ученых и специалистов из различных областей знаний к экономическим, финансовым, математическим, техническим и иным проблемам цифровой трансформации.

Нашедшие отражение в многотомном издании 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, включая разработчиков и производителей продуктов на основе достижений цифровых технологий, молодым исследователям-студентам, магистрантам и аспирантам, всем интересующимся вопросами взаимовлияния цифровых технологий и права.

УДК 004:34(063)
ББК 67с51я43

ISBN 978-5-8399-0859-8

ISBN 978-5-8399-0843-7 (Vol. 3)

© Авторы статей, 2024

© Казанский инновационный университет
имени В. Г. Тимирязова, 2024

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов II Международной научно-практической конференции

20 сентября 2024 г.
г. Казань

В шести томах
Том 3

Под редакцией И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой

Электронное издание

Главный редактор Г. Я. Дарчинова; редакторы: Г. А. Тарасова, Е. А. Маннапова;
технические редакторы: О. А. Аймурзаева, С. Р. Каримова; дизайн обложки: Г. И. Заретдинова

Дата подписания к использованию: 13.12.2024. Объем издания 5,3 Мб. Тираж 11 экз. Заказ № 10/2024.
ISBN 978-5-8399-0843-7

Издательство Казанского инновационного университета им. В. Г. Тимирязова
420111, г. Казань, ул. Московская, 42 Тел. (843) 231-92-90, E-mail: zaharova@icml.ru



UDC 004:34(063)
LBC 67c51я43

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

Reviewers:

A. K. Zharova, Dr. Sci. (Law), Associate Professor, Director of the Center for Cyberspace Research, Associate Member of the International Scientific and Educational Center “UNESCO Chair in Copyright, Related, Cultural and Information Rights” of the National Research University Higher School of Economics;

K. A. Ponomareva, Dr. Sci. (Law), Associate Professor, Leading Researcher of Centre for Taxation Policy of Scientific-research Institute of the Russian Ministry of Finance, Professor of the Department of Legal Provision of Market Economy, Higher School of Legal Studies, Russian Presidential Academy of National Economy and Public Administration;

E. A. Russkevich, Dr. Sci. (Law), Associate Professor, Professor of the Department of Criminal Law of the Moscow State Law University named after O. E. Kutafin;

K. L. Tomashevsky, Dr. Sci. (Law), Professor, Deputy Dean of the Faculty of Law for Research, Professor of the Department of Civil and Business Law of the Kazan Innovation University named after V. G. Timiryasov;

Yu. S. Kharitonova, Dr. Sci. (Law), Professor, Head of the Center for Legal Research of Artificial Intelligence and Digital Economy, Professor of the Department of Business Law at Lomonosov Moscow State University

Digital Technologies and Law: collection of scientific papers of the III International Scientific and Practical Conference (Kazan, 2024, September 20) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 3. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2024. EDN: QONPHL. http://dx.doi.org/10.21202/978-5-8399-0843-7_3 – 1 CD-ROM. – Title from the title screen. – Text: electronic.

ISBN 978-5-8399-0859-8

ISBN 978-5-8399-0843-7 (Vol. 3)

System requirements: Linux, Windows operation systems; 120 Mb; 16 Mb; PDF Reader; CD-ROM, mouse

The scientific works included in this collection are timed to coincide with the III International Scientific and Practical Conference “Digital Technologies and Law”, held on September 20, 2024 in Kazan as part of the International Forum “Kazan Digital Week 2024”, organized by the Government of the Russian Federation jointly with the Cabinet of Ministers of the Republic of Tatarstan.

The conference discussed a wide range of theoretical, methodological, practice-oriented, interdisciplinary and sectoral issues related to the development priorities of legal regulation in the sphere of digital technologies, regulatory control over the digital environment, prospects for the influence of law on the formation and development of new public relations.

The scientific works in this volume are systematized according to modern trends in the development of digital technologies within the system of criminal-legal relations. The views and approaches of scientists and specialists from various fields of knowledge concerning the economic, financial, mathematical, technical and other issues of digital transformation are summarized separately in the format of a multidisciplinary “hackathon”.

Taken together, the ideas and proposals reflected in this multi-volume publication are the key to understanding the intellectual map of meanings that will be of interest to legal scholars and experts in the field of digital technologies; practicing lawyers; representatives of law-making and law enforcement agencies; civil servants and participants in the real sector of the economy, including developers and manufacturers of products based on digital technologies; to young researchers: undergraduates, graduates, and postgraduates; to all those interested in the mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67c51я43

ISBN 978-5-8399-0859-8

ISBN 978-5-8399-0843-7 (Vol. 3)

© Authors of articles, 2024

© Kazan Innovative University
named after V. G. Timiryasov, 2024

Scientific publication

DIGITAL TECHNOLOGIES AND LAW

Collection of scientific papers of the III International Scientific and Practical Conference

2024 September 20
Kazan

In 6 volumes

Volume 3

I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.)

Electronic publication

Editor-in-Chief G. Ya. Darchinova; Editors G. A. Tarasova, E. A. Mannapova;
Technical Editors O. A. Aimurzaeva, S. A. Karimova; Cover designer G. I. Zagretdinova

Date of signing for usage: 13.12.2024. Volume of the publication 5.3 Mb. Number of copies: 11. Order No. 10/2024.
ISBN 978-5-8399-0843-7

Poznaniye Publishing House of Kazan Innovative University named after V. G. Timiryasov
42 Moskovskaya Str., 420111 Kazan, Russian Federation; Tel. +7 (843) 231-92-90; E-mail: zaharova@ieml.ru



Редакторы:

И. Р. Бегиев, доктор юридических наук, доцент, 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, доктор юридических наук, доцент, заместитель директора Юридического института по международной деятельности, профессор кафедры гражданского права и гражданского судопроизводства Южно-Уральского государственного университета (национального исследовательского 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. Шутова, 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

Editors:

I. R. Begishev, Dr. Sci. (Law), Associate Professor, Honored Lawyer of the Republic of Tatarstan, Chief Researcher of the Research Institute of Digital Technologies and Law, Professor of the Department of Criminal Law and Process of the Kazan Innovation University named after V. G. Timiryasov;

E. A. Gromova, Dr. Sci. (Law), Associate Professor, Deputy Director on international activity of the Institute of Law, Professor of the Department of Civil Law and Procedure, South Ural State University (national research university);

M. V. Zaloilo, Cand. Sci. (Law), leading researcher at the Department of Theory of Law and Interdisciplinary Research of Legislation at the Institute of Legislation and Comparative Law under the Government of the Russian Federation;

I. A. Filipova, Cand. Sci. (Law), Associate Professor, Associate Professor of the Department of Labor and Environmental Law of the National Research Nizhny Novgorod State University named after N. I. Lobachevsky;

A. A. Shutova, Cand. Sci. (Law), senior researcher at the Research Institute of Digital Technologies and Law, associate professor of the department of criminal law and process of the Kazan Innovation University named after V. G. Timiryasov

СОДЕРЖАНИЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЙ

Алексеева Т. С. СОЗДАНИЕ ДИПФЕЙКОВ КАК ПРЕСТУПЛЕНИЕ ПРОТИВ ЛИЧНОСТИ....	11
Антонова Е. Ю. ВОВЛЕЧЕНИЕ В ТЕРРОРИСТИЧЕСКУЮ, ЭКСТРЕМИСТСКУЮ И ДИВЕРСИОННУЮ ДЕЯТЕЛЬНОСТЬ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ: УГОЛОВНО-ПОЛИТИЧЕСКИЙ АСПЕКТ	14
Бегишев И. Р., Денисов Н. Л. ПРОБЛЕМЫ КРИМИНОЛОГИЧЕСКОГО ИЗУЧЕНИЯ И АНАЛИЗА ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБОРОТА ЦИФРОВОЙ ВАЛЮТЫ.....	24
Бегишев И. Р., Хусаинов А. А. СОДЕРЖАНИЕ И ТЕНДЕНЦИИ ЦИФРОВОЙ ПРЕСТУПНОСТИ.....	27
Вальтер А. В., Гончаров Д. Ю. ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ ДЛЯ ЭВМ «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ПРОТИВОДЕЙСТВИЯ НАЛОГОВЫМ ПРЕСТУПЛЕНИЯМ» И ПЕРСПЕКТИВЫ ЕЕ ПРИМЕНЕНИЯ	29
Власова Е. Л., Глезова А. Д. ПРОТИВОДЕЙСВИЕ КИБЕРПРЕСТУПЛЕНИЯМ КАК ОСНОВНАЯ ПРОБЛЕМА В СОВРЕМЕННОМ ОБЩЕСТВЕ	33
Гильманов Э. М., Бабаева А. М. ИСПОЛЬЗОВАНИЕ КРИМИНАЛИСТИЧЕСКИХ МЕТОДИК ДЛЯ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В ЦИФРОВОЙ СФЕРЕ	36
Гильманов Э. М., Гильманов Р. Э., Азаров Э. Е. ОТВЕТСТВЕННОСТЬ ЗА РАСКРЫТИЕ ПОСРЕДСТВОМ СЕТИ ИНТЕРНЕТ ДАННЫХ, СТАВШИХ ИЗВЕСТНЫМИ В ХОДЕ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ.....	39
Глянц Е. М. ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНИХ В ПРЕСТУПНУЮ ДЕЯТЕЛЬНОСТЬ ПОСРЕДСТВОМ ВЗАИМОДЕЙСТВИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ.	42
Графова Ю. М. СИСТЕМА ПРОФИЛАКТИКИ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ.....	46
Денисович В. В. КРИМИНОЛОГИЧЕСКИЕ И ЭТИЧЕСКИЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ МЕТАВСЕЛЕННЫХ	48
Денисович В. В. КРИМИНОЛОГИЧЕСКОЕ ИЗМЕРЕНИЕ МЕТАВСЕЛЕННЫХ	51
Дроздов Д. Е. ЦИФРОВЫЕ СРЕДСТВА ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПНОСТИ.....	56
Дубынин Е. А., Берняцкий А. А. ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНОМ ПРОЦЕССУАЛЬНОМ ПРАВЕ	59
Дударев В. А. СОВРЕМЕННЫЕ ЦИФРОВЫЕ ТЕХНОЛОГИИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ	65
Ефимов Е. В. СООТНОШЕНИЕ СРЕДСТВ ДОКАЗЫВАНИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ И РЕЗУЛЬТАТОВ РАБОТЫ АЛГОРИТМОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА	69
Иванова Л. В. ДИФФЕРЕНЦИАЦИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ В СФЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И РОБОТОТЕХНИКИ: ПОСТАНОВКА ПРОБЛЕМЫ..	74

Креховец А. В. ЗАРУБЕЖНЫЙ И РОССИЙСКИЙ ОПЫТ В УГОЛОВНО-ПРАВОВОЙ РЕГЛАМЕНТАЦИИ ОТВЕТСТВЕННОСТИ ЗА ТРЕШ-СТРИМЫ.....	77
Кукеев А. К. ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИХ РОЛЬ В ПОВЫШЕНИИ ПРОЗРАЧНОСТИ И ЭФФЕКТИВНОСТИ АНТИКОРРУПЦИОННЫХ МЕРОПРИЯТИЙ.....	80
Латыпова Э. Ю., Мусина Р. Р. О НОВОМ КВАЛИФИЦИРУЮЩЕМ ПРИЗНАКЕ В ОСОБЕННОЙ ЧАСТИ УК РФ – ПУБЛИЧНОЙ ДЕМОНСТРАЦИИ ПОСРЕДСТВОМ СМИ.....	85
Латыпова Э. Ю., Рогова К. М. О ПРОЦЕССЕ ПРИЗНАНИЯ ЛИЦА ИНОСТРАННЫМ АГЕНТОМ	88
Лобач Д. В. УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПУБЛИЧНЫЕ ПРИЗЫВЫ К АГРЕССИВНОЙ ВОЙНЕ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОСТОЯНИЯ: ПЕРСПЕКТИВА МОДЕРНИЗАЦИИ	94
Лопатина Т. М. НАУЧНО-ТЕХНИЧЕСКИЙ ПРОГРЕСС КАК ФАКТОР ТРАНСФОРМАЦИИ УГОЛОВНОГО ПРАВА	101
Малышева Ю. Ю. УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ ВЗЯТКИ И ПОДАРКА В ЦИФРОВОМ ПРОСТРАНСТВЕ	107
Малышкин Р. Н. ЭЛЕКТРОННОЕ (ЦИФРОВОЕ) УГОЛОВНОЕ ДЕЛО: НЕИЗБЕЖНАЯ РЕАЛЬНОСТЬ	112
Маркелов А. Г. ПРАВО НА ТЕЛЕФОННЫЙ РАЗГОВОР В УГОЛОВНОМ ПРОЦЕССЕ РОССИИ ОСТАЕТСЯ НЕРАЗРЕШЕННОЙ	119
Никитина И. Э. ВЗАИМОДЕЙСТВИЕ ГОСУДАРСТВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И ПРАВА ЧЕЛОВЕКА...	124
Петрикина А. А. ЦИФРОВЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ УДЕБНОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ	128
Петров П. К. ЦИФРОВИЗАЦИЯ УГОЛОВНОГО СУДОПРОИЗВОДСТВА: ПРОБЛЕМЫ ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ.....	131
Петров П. К. ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ И ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В МЕТОДИКЕ ЗАЩИТЫ ПО УГОЛОВНЫМ ДЕЛАМ.....	134
Радченко Т. В. ПРАВОВЫЕ И ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ДЕТЕРМИНАЦИИ ТЕРМИНОЛОГИЧЕСКОГО АППАРАТА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ КВАЛИФИКАЦИИ	137
Реховский А. Ф. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В УГОЛОВНОМ ПРАВОСУДИИ: АНАЛИЗ ОГРАНИЧЕНИЙ И ЭТИЧЕСКИХ ВЫЗОВОВ В СВЕТЕ ЕВРОПЕЙСКОГО ЗАКОНА ОБ ИСКУССТВЕННОМ ИНТЕЛЛЕКТЕ.....	144
Романов В. И. К ВОПРОСУ О ЦИФРОВИЗАЦИИ В РАБОТЕ СЛЕДОВАТЕЛЯ.....	150
Колесников Р. В., Сенцов В. В. РОЛЬ «КРИПТОВАЛЮТЫ» В УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЯХ	152
Силаева Н. А. ПОЛИЦИЯ КАК СУБЪЕКТ ПРОФИЛАКТИКИ И ЗАЩИТЫ ОТ КРИМИНАЛЬНОЙ ВИКТИМНОСТИ ИНВАЛИДОВ В УСЛОВИЯХ ЦИФРОВОГО ОБЩЕСТВА.....	156

Малышкин Р. Н., Слепнева И. В. О ВОПРОСАХ КВАЛИФИКАЦИИ КРАЖИ С БАНКОВСКОГО СЧЕТА, А РАВНО В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ.....	161
Хайрутдинова Л. Р. ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ КВАЛИФИКАЦИИ И ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ КИБЕРГРУМИНГА КАК ПРЕСТУПЛЕНИЯ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ НЕСОВЕРШЕННОЛЕТНИХ	165
Шутова А. А. КОНЦЕПЦИЯ ЦИФРОВОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ КАК ФЕНОМЕНА, ЗНАЧИМОГО ДЛЯ УГОЛОВНОГО ПРАВА	168

МУЛЬТИДИСЦИПЛИНАРНЫЕ (НЕЮРИДИЧЕСКИЕ) АСПЕКТЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аникеева В.-М. Д., Кочеткова О. В. ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ РАЗРАБОТКИ ЭКСПЕРТНОЙ СИСТЕМЫ ПО ПОДДЕРЖКЕ ПРИНЯТИЯ РЕШЕНИЙ ПО ПЕРЕВОДУ ГОСУДАРСТВЕННЫХ УСЛУГ В ЭЛЕКТРОННУЮ ФОРМУ ПРЕДСТАВЛЕНИЯ	179
Артюшкин В. Ф., Гусева Е. А., Ибрагимова Е. Ю. АНАЛИЗ СТАТИСТИКИ ПРЕСТУПНОСТИ ПО МЕТОДИКЕ ВИЗУАЛИЗАЦИИ МНОГОМЕРНЫХ СТРУКТУР.....	194
Беляева А. А. ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ДЛЯ ПОСТРОЕНИЯ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ДИНАМИКИ ЭЛЕКТРОНОВ В СИНХРОТРОНЕ	204
Богданова О. В. СЕЛЕКЦИЯ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ	212
Вербицкая Т. В. ПРОБЛЕМЫ ФОРМИРОВАНИЯ МЕХАНИЗМА ЗАЩИТЫ ОТ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ В ОТНОШЕНИИ ЦИФРОВЫХ КОПИЙ АРХИВНЫХ ДОКУМЕНТОВ, РАЗМЕЩЕННЫХ В СЕТИ ИНТЕРНЕТ	217
Вишнякова Е. Д., Кочеткова О. В. ИССЛЕДОВАНИЕ ПРОЦЕССА КОНТРОЛЯ РАБОТОСПОСОБНОСТИ ИНТЕГРАЦИИ ДАННЫХ В ДЕЯТЕЛЬНОСТИ СИТУАЦИОННОГО ЦЕНТРА ГУБЕРНАТОРА ВОЛГОГРАДСКОЙ ОБЛАСТИ.....	222
Дубовикова Е. М., Егоров Г. Г. ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ НЕЙРОСЕТЕЙ ПРИ ИЗУЧЕНИИ АНГЛИЙСКОГО ЯЗЫКА.....	246
Киселкина О. В. РАЗВИТИЕ ЦИФРОВИЗАЦИИ РЕКРУТМЕНТА.....	251
Кочеткова О. В., Вольф С. В., Беликова Е. А. ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ЭФФЕКТИВНОГО ЛЕЧЕНИЯ ПАЦИЕНТОВ С ХРОНИЧЕСКИМ ГЕПАТИТОМ С	254
Кружалова Л. В. ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ХУДОЖЕСТВЕННОЙ ЛИТЕРАТУРЫ И ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРЕПОДАВАНИИ КОНФЛИКТОЛОГИИ.....	257
Куркова Н. А., Макарова О. А. АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ЦИФРОВЫХ СЕРВИСОВ В ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ.....	263
Лаврёнов А. Н. ПРАВО В РАМКАХ «ПСИХОЛОГИЗАЦИИ» ОБЩЕСТВА И ОБРАЗОВАНИЯ.....	269
Огуенко В. В. КАРТОГРАФИРОВАНИЕ С ПОМОЩЬЮ ДРОНОВ.....	273
Ризаев И. И. ВЛИЯНИЕ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ НА ОБРАЗОВАНИЕ И ПСИХОЛОГИЮ ДЕТЕЙ: СОЦИАЛЬНО-ФИЛОСОФСКИЙ АНАЛИЗ	275

Романова А. С. МОДЕЛИРОВАНИЕ АВТОНОМНЫХ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УПРАВЛЕНИЯ КОРПОРАЦИЯМИ	281
Сайдашева В. А. НЕКОТОРЫЕ АСПЕКТЫ ЦИФРОВИЗАЦИИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ НА СТАДИИ ВОЗВРАТА ТОВАРОВ	288
Селиверстова Н. С., Григорьева О. В. СУЩЕСТВЕННЫЕ И ЧАСТНЫЕ ПРИЗНАКИ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ КАК КОНВЕРГЕНТНОГО ФАКТОРА СТРУКТУРНЫХ СДВИГОВ	292
Сметанин Ю. М., Сметанина В. М., Бусоргин Г. А. ВЕРИФИКАЦИЯ ВЕРСИЙ РАССЛЕДОВАНИЯ НА ОСНОВЕ КОМПЬЮТЕРНОЙ ЛОГИКО-СЕМАНТИЧЕСКОЙ МОДЕЛИ.....	296
Хмелев А. В., Матюнин Д. Д., Попова Е. В. ЦИФРОВЫЕ СЕРВИСЫ КАК ИНСТРУМЕНТ ДЛЯ ПОИСКА АЛЬТЕРНАТИВНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ТЕКУЩИХ РЕАЛИЯХ	303
Хмелев А. В., Толстиков А. С. К ВОПРОСУ ВНЕДРЕНИЯ ИНТЕРАКТИВНЫХ ЭЛЕМЕНТОВ В СЛОЖНЫЕ САЙТЫ С ЦЕЛЬЮ ПОМОЩИ ПОЛЬЗОВАТЕЛЮ	306
Шаймиева Э. Ш., Гумерова Г. И. СОБЫТИЙНЫЙ БРЕНД КРЕАТИВНЫХ ИНДУСТРИЙ В ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ, СТАРТАП-ДВИЖЕНИИ	309

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ТЕОРЕТИКО-ИСТОРИЧЕСКИХ ПРАВОВЫХ НАУК

Т. С. Алексеева,

аспирант,

Московский государственный университет

имени М. В. Ломоносова,

юрист,

Аналитический центр уголовного права и криминологии

СОЗДАНИЕ ДИПФЕЙКОВ КАК ПРЕСТУПЛЕНИЕ ПРОТИВ ЛИЧНОСТИ

Аннотация. В статье обозначены аспекты использования технологии дипфейков: они могут быть использованы для совершения различных преступлений, но способны причинить существенный вред личности. Частично он охвачен нормой о клевете, частично – оборотом порнографических материалов, но и то, и другое оставляет вне уголовно-правового поля ряд общественно опасных действий с интимными изображениями. Это обуславливает необходимость уточнения в нормы уголовного закона.

Ключевые слова: уголовное право, дипфейк, изображение человека, личная тайна, порнография, компьютерная информация, изготовление

CREATION OF DEEPPFAKES AS THE OFFENSE AGAINST THE PERSON

Abstract. The article covers usage of deepfake technologies. They may be used to commit various crimes, but can lead to serious harm to a person. This harm is partly covered by provisions on libel and pornography, but both of them leave certain acts with intimate images out of the criminal law field. This is why some criminal law provisions need to be modified.

Keywords: criminal law, deepfake, personal image, personal secrecy, pornography, computer information, production

Введение. Выбор темы, обозначенной в заглавии статьи, предопределен несколькими факторами: среди них общее распространение технологий изменения изображений, потенциальное достижение высокой степени их достоверности, сбор и использование биометрических персональных данных различными организациями. Риски неправомерного использования изображения и голосовых образцов повышаются в связи с большим количеством данных, доступных для неопределенного круга лиц в социальных сетях.

Тем не менее уголовное право, будучи по своей природе *ultima ratio*, не является приоритетным выбором при конструировании механизма защиты права на изображение, а потому при постановке вопроса об уголовно-правовой защите от дипфейков следует решить, во-первых, *когда* нужно задействовать уголовно-

правовой механизм, во-вторых – *какой объект* защищается в данном случае, в-третьих – *какое действие* в отношении *какого предмета* должно лежать в основе объективной стороны состава.

Защита личности от дипфейков: когда и почему? В контексте дипфейков внимание законодателей рано привлекло использование подобных материалов для влияния на политические процессы (в частности, механизм защиты от таких действий создан во многих штатах США) [2. С. 374–375]. Многообразны правомерные варианты использования (в культурных, образовательных, рекламных и прочих целях, а также в рамках реализации свободы выражения мнений, при условии соблюдении законодательных ограничений и прав других лиц).

Тем не менее лицу, зафиксированному на сгенерированном изображении, может быть причинен вред, достаточный для уголовно-правового вмешательства и различный по своей правовой природе. Неверное впечатление, сформированное голосом или изображением, способно причинить вред, в первую очередь, чести и достоинству, но также идентичности лица, его контролю над информацией о себе, иными словами – неприкосновенности частной жизни в ее широком понимании.

Это нередко часть единой линии поведения, которая может быть совершена и с небольшим объемом сведений о человеке; технология дипфейков способна повысить достоверность информации, размещаемой от имени другого лица. Иллюстрации варьируются от простого использования чужого изображения для аватара [см., напр., 4] до объявлений на сайтах знакомств, с адресом и номером телефона, провоцирующих соответствующее сексуальное поведение в адрес потерпевшего [6. С. 79].

Создание ложного впечатления о человеке в отдельных случаях соответствует признакам клеветы, при условии определенной конкретизации сведений: если имеется в виду видеоизображение, легко представить сведения, которые могут быть почерпнуты из него (напр., «сгенерированный» процесс дачи или получения взятки, что однозначно относится к сведениям, порочащим честь и достоинство). Статичное изображение человека с меньшей вероятностью отражает информацию, которая может быть признана фактической.

«Ассортимент» объектов: критерии выбора. Отвечая на вопрос, какие нормы могут защитить от общественно опасных дипфейков, исследователи очень часто называют клевету и незаконный оборот порнографической продукции. Применительно к клевете, как было отмечено выше, нет принципиально новых проблем квалификации. Изображение или голос отличаются повышенной достоверностью в глазах окружающих, это «второй уровень ложности» [7. С. 433], но признаки состава от этого не нуждаются в уточнении. Между тем далеко не все изображения, приносящие вред, могут быть предметом клеветы: например, сами по себе интимные фотографии не содержат порочащих сведений, если не указывают на связь с конкретным лицом для определенных порочащих целей.

Применительно к порнографии отмечается, что «действующая редакция ст. 242 УК РФ позволяет квалифицировать так называемый FaceSwar <...> как изготовление порнографических материалов» [3. С. 100]. Соглашаясь с этим утверждением, отмечу, что квалификация создания дипфейка в качестве изготовления порнографического материала не решает проблемы защиты личности: изображенный не становится потерпевшим.

Изображение является предметом нескольких составов преступлений против личности. Для защиты права на изображение актуальнее всего, помимо клеветы, ст. 137 УК РФ («Нарушение неприкосновенности частной жизни»): ее диспозиция не содержит упоминания изображений, но охватывает случаи, когда изображения являются личной тайной. Наиболее яркая иллюстрация – интимные изображения, которые нередко получены законно (по согласию изображенного лица), но впоследствии распространены по мотиву ревности, в результате возникновения личных неприязненных отношений. Предмет ст. 137 УК РФ также показывает, почему оборот порнографии не может защитить личность: часть действий, которые квалифицируются как распространение личной тайны, не являются распространением порнографических материалов, по результатам искусствоведческих экспертиз (см., напр., Кассационное определение Второго КСОЮ от 2 марта 2021 г. № 77-566/2021: одна из интимных фотографий потерпевших – порнографическая).

Сгенерированные изображения предметом ст. 137 УК РФ быть не могут: тайной является исключительно информация, соответствующая действительности. С той же проблемой столкнулись правовые порядки, в которых в норме о защите частной жизни изображения были обособлены: в частности, Уголовным кодексом Испании интимные изображения защищены в ст. 197, однако эта норма охватывает исключительно действительные изображения – дипфейки вне ее действия [8. С. 6–7].

Предмет и действия с ним, или основы построения составов. Дипфейки – как результат и первичный образец, как материал для такого результата – с позиции уголовного закона в самом общем виде могут быть описаны как определенные «сведения», «информация». К дипфейкам будет применим и термин «компьютерная информация»; едва ли при этом можно согласиться с тем, что именно она является основным объектом при любом использовании технологии.

Для исследователей бланкетного регулирования после вывода, что внешность и голос не защищаются авторским правом, неизбежен переход к анализу режима персональных и, в частности, биометрических данных [1. С. 115–116]. Хотя и изображения, и образец голоса в целом к таковым относятся, для них применимо требование идентификации лица: далеко не любое изображение может установить личность (именно поэтому по ряду дел по ст. 137 УК РФ сторона защиты ссылается на то, что часть распространенных изображений не идентифицирует потерпевшего, см., напр.: Апелляционное определение Новосибирского областного суда от 14 января 2022 г. по делу № 22-7540/2021).

Представляется, что изображение и голос могут быть названы в норме именно таким образом, без отсылки к персональным данным; что же касается деяния, то в действующем уголовном законе есть «модификация» [компьютерной информации], «изготовление» [порнографических материалов], «создание» [компьютерных программ]. Будут ли они достаточны для криминализации? Если в основе результата лежит законно полученное изображение лица, которое превращено в интимное с помощью технологий и оставлено создателем для личного пользования, то общественная опасность отсутствует. Однако использование (напр., для шантажа) и распространение могут причинить существенный вред личности.

Заключение. Для многих составов дипфейк – средство, которое по усмотрению законодателя может «заслужить» квалифицирующий признак (как в разрабатываемом законопроекте) [5]. Однако дипфейк, содержащий интимные сведения, играет немалую роль для причинения вреда частной жизни, неприкосновенности лица, а потому заслуживают внимания использование изготовленного изображения в неправомерных целях, распространение подобных изображений.

Список литературы

1. Добробаба М. Б. Дипфейки как угроза правам человека // Lex russica. 2022. Т. 75, № 11. С. 112–119.
2. Дремлюга Р. И., Коробеев А. И. Борьба с распространением реалистичных аудиовизуальных поддельных материалов за рубежом (deepfake): уголовно-правовые и криминологические аспекты // Всероссийский криминологический журнал. 2021. Т. 15, № 3. С. 372–379.
3. Ефремова М. А., Русскевич Е. А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 2 (56). С. 97–105.
4. Береги фейс смолоду // Блог KasperskyDaily. URL: <https://www.kaspersky.ru/blog/findface-experiment/11671> (дата обращения: 06.09.2024).
5. В Госдуме назвали возможный срок внесения законопроекта о дипфейках // URL: www.gazeta.tu/social/news/2024/09/08/23878183.shtml?updated (дата обращения: 08.09.2024).
6. Филатова М. А. Уголовная ответственность за киберсталкинг // Уголовное право. 2020. № 4. С. 77–82.
7. Garon Jon M. An AI's Picture Paints A Thousand Lies: Designating Responsibility for Visual Libel // Journal of Free Speech Law. 2023. No. 3. P. 425–454.
8. Jareño Leal, Ángeles. El derecho a la imagen íntima y el Código penal. La calificación de los casos de elaboración y difusión del deepfake sexual // Revista Electrónica de Ciencia Penal y Criminología. 2024. Núm. 26–09. Pp. 1–37.

Е. Ю. Антонова,

доктор юридических наук, профессор,
Университет прокуратуры Российской Федерации,
Дальневосточный юридический институт (филиал)

ВОВЛЕЧЕНИЕ В ТЕРРОРИСТИЧЕСКУЮ, ЭКСТРЕМИСТСКУЮ И ДИВЕРСИОННУЮ ДЕЯТЕЛЬНОСТЬ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ: УГОЛОВНО-ПОЛИТИЧЕСКИЙ АСПЕКТ

Аннотация. В статье рассматриваются отдельные уголовно-политические вопросы о мерах правового воздействия на субъекты, вовлекающие (склоняющие, вербующие) других лиц в совершение преступлений террористического характера, экстремистской или диверсионной направленности с использованием цифровых технологий. Раскрываются общественная опасность и механизм совершения таких преступлений. Определено, что цифровые технологии исполь-

зуются в процессе выполнения их объективной стороны. Делается вывод о необходимости корректировки уголовного закона.

Ключевые слова: уголовная политика, терроризм, экстремизм, диверсионная деятельность, склонение, вербовка, информационно-телекоммуникационные сети (ИТС), информационно-телекоммуникационные технологии (ИТТ), Интернет, пропаганда идеологии

INVOLVEMENT IN TERRORIST AND EXTREMIST ACTIVITIES USING DIGITAL TECHNOLOGIES: THE CRIMINAL-POLITICAL ASPECT

Abstract. The article examines individual criminal-political issues on measures of legal influence on subjects who involve (incline, recruit) other persons in committing crimes of a terrorist, extremist or sabotage nature using digital technologies. The social danger and the mechanism for committing such crimes are revealed. It has been determined that digital technologies are used in the process of performing their objective side. The conclusion is made about the need to adjust the criminal law.

Keywords: criminal policy, terrorism, extremism, sabotage, inducement, recruitment, information and telecommunication networks, information and telecommunication technologies, Internet, ideological propaganda

Введение. В последние годы отмечается рост террористических, экстремистских и диверсионных преступлений. Так, по данным государственной статистической отчетности, в 2018 г. было зарегистрировано 1 679 террористических преступлений, 1 265 – экстремистских и 1 факт диверсии; в 2019 г. – 1 806, 585 и 0; в 2020 г. – 2 342, 833 и 0; в 2021 г. – 2 136, 1 057 и 1; в 2022 г. – 2 233, 1 566 и 23 соответственно; в 2023 г. – 2 382 террористических преступления, 1 340 экстремистских и 188 диверсионных преступлений (из них 154 факта диверсий).

При этом очевидно, что терроризм, экстремизм и диверсионная деятельность характеризуются организованностью. Террористическим/ экстремистским/диверсионным формированиям требуется непрерывное пополнение членами, руководствующимися соответствующей идеологией. Это порождает и проблему противодействия вовлечению лиц в совершение преступлений террористической, экстремистской и диверсионной направленности. Ситуация усугубляется тем, что террористические, экстремистские и диверсионные формирования все больше используют различные цифровые площадки для радикализации не только взрослых, но и несовершеннолетних лиц.

Неблагоприятная динамика использования цифровых технологий в процессе вовлечения (склонения, вербовки) лиц в совершение названных преступлений обусловлена целым рядом детерминант. Среди таковых можно выделить, например, латентность преступлений, совершаемых с использованием ИТТ, несовершенство мер уголовно-правового реагирования на факты совершаемых соответствующим образом общественно опасных деяний и механизма их учета, легкая доступность деструктивного контента на цифровых площадках, недостаточный уровень цифровых знаний у населения и фактической раскрываемости таких преступлений.

Отсюда возникают вопросы об эффективности уголовно-правовой политики государства в части минимизации количества преступлений, направленных на вовлечение лиц в совершение таких преступлений.

Постановка проблемы. Анализ уголовного закона показывает, что законодатель криминализировал уже достаточное количество деяний, которые способствуют такому вовлечению. В частности, выделены в уголовном законе нормы о вовлечении (склонении, вербовке) лиц в совершение террористического преступления (ч. 1, 1¹ ст. 205¹) и диверсии (ч. 1 ст. 281¹), в деятельность экстремистского сообщества (ч. 1¹ ст. 282¹) или экстремистской организации (ч. 1¹ ст. 282²).

При этом в названных составах преступлений не предусмотрен такой криминообразующий или отягчающий признак, как совершение таковых «с использованием ИТС, включая сеть “Интернет”».

Названные преступления также способствуют вовлечению лиц в совершение рассматриваемых преступлений, но соответствующие призывы воздействуют на неопределенно широкий круг лиц, тогда как вовлечение (склонение, вербовка) связано с воздействием на конкретное лицо или группы лиц.

Широкий спектр контента, создаваемого террористическими, экстремистскими, диверсионными формированиями, считается незаконным во многих странах, как и формальное или неформальное членство в них. Это создает дилемму для этих формирований, действующих на различных цифровых площадках: высокий уровень секретности может быть достигнут с помощью шифрования, тем самым минимизируя риск обнаружения, но это серьезно ограничивает охват рекрутов и сочувствующих. Кроме того, доступность экстремистских материалов на цифровых площадках может быть очень высокой, но цифровые файлы оставляют следы на устройствах отдельных лиц, и простая загрузка определенных материалов может привести к обнаружению и судебному преследованию. В результате указанные формирования демонстрируют значительную адаптивность и гибкость в использовании онлайн-сервисов и платформ. Общая стратегия, разработанная за последние несколько лет, заключается в использовании точек входа на основных сайтах, которые можно использовать для направления заинтересованных лиц в другие цифровые места, такие как зашифрованные сервисы или специализированные веб-сайты [15].

Анализ судебной практики подтверждает факт того, что вовлечение (склонение, вербовка) лиц в террористическую, экстремистскую или диверсионную деятельность зачастую совершаются с применением цифровых технологий, что отражено и в Доктрине информационной безопасности [1].

Так, Г., с целью склонения и вовлечения российских граждан в террористическую деятельность на территории Сирии, стал вести переписку с С-вым в электронном приложении мобильного телефона, разъясняя ему основы радикального ислама. Кроме того, Г. направил С-ву посредством этого же электронного приложения видеозаписи (6), графические файлы (7) и аудиофайлы (4) с материалами, описывающими образ «врага» неисламских правительств, формирующими желание и укрепляющими решимость совершать террористические действия, и содержащими радикальную информацию [4].

В апреле 2023 г. 20-летний мужчина разместил на одном из сайтов в сети «Интернет» объявление о поиске подработки, оставив свои контактные данные. Через некоторое время он получил сообщение в мессенджере от неустановленного пользователя, который предложил ему заработать денег, поджигая объекты железнодорожной транспортной инфраструктуры, а также порекомендовал найти соучастников, за что можно было получить дополнительное денежное вознаграждение. Мужчину данное предложение заинтересовало, он предпринял действия по поиску сообщников и орудий преступления [9].

И таких примеров можно привести еще очень много.

Отметим, что некоторые зарубежные страны установили повышенную уголовную ответственность за использование цифровых технологий при вовлечении лица в совершение террористических, экстремистских и диверсионных преступлений. Например, п. «г» ч. 2 ст. 179(1) УК Республики Таджикистан [13] предусматривает квалифицирующий признак «с использованием СМИ или сети Интернет» при вовлечении лиц в совершение террористических преступлений.

Отсюда возникает потребность в решении вопроса об изменении интенсивности пенализации в составах преступлений, в которых идет речь о склонении, вербовке или вовлечении лиц в террористическую, экстремистскую или диверсионную деятельность путем установления квалифицирующего признака – совершение преступления «с использованием ИТС, включая сеть “Интернет”».

Основания изменения интенсивности пенализации. Базовыми критериями криминализации деяния и изменения интенсивности их пенализации являются общественная опасность деяния и его относительная распространенность.

Если рассматривать вовлечение (склонение, вербовку) лиц в террористические, экстремистские и диверсионные преступления, становится очевидным, что такие деяния имеют высокую степень общественной опасности, относительно распространенными являются и случаи их совершения с использованием цифровых технологий. Так, по данным статистики, в 2019 г. – 122 (31 – 25,4%) и 26 (12 – 46,2%); в 2020 г. – 72 (21 – 29,2%) и 49 (20 – 40,8%); в 2021 г. – 94 (27 – 28,7%) и 61 (21 – 34,4); в 2022 г. – 66 (19 – 28,8%) и 49 (20 – 40,8%); в 2023 г. – 38 (23 – 60,5%) и 46 (19 – 41,3%) соответственно.

Кроме того, в 2018 г. зарегистрировано 4 преступления, предусмотренных ч. 1¹ ст. 282¹ УК РФ (из них 1 – 25% с использованием сети «Интернет»), и 5 преступлений, предусмотренных ч. 1¹ ст. 282² УК РФ (из них 0 с использованием сети «Интернет»); в 2019 г. – 1 (0) и 13 (0); в 2020 г. – 5 (2 – 40%) и 26 (1 – 3,8%); в 2021 г. – 4 (1 – 25%) и 49 (14 – 28,6%); в 2022 г. – 5 (1 – 20%); в 2023 г. – 1 (0) и 27 (6 – 22,2%).

Представленные данные подтверждают тот факт, что вовлечение (склонение, вербовка) лиц в совершение рассматриваемых преступлений с использованием ИТС является относительно распространенным, т.е. типичным, а не случайным или редким.

Говоря об общественной опасности рассматриваемых преступлений, отметим, что цифровые технологии пронизывают все аспекты нашей жизни. И, конечно же, террористические, экстремистские и диверсионные формирования идут в ногу с научно-техническим прогрессом в сфере цифровых коммуни-

каций. Уже сегодня становится понятным, что онлайн и офлайн-коммуникации усиливают друг друга, что оказывает существенную роль в вербовке новых участников противоправной деятельности.

При этом очевидно, что для терроризма, экстремизма и диверсионной деятельности характерна идеология насилия [2. С. 69–74]. В связи с этим лица, вовлекающие в рассматриваемые виды преступной деятельности новых участников, в первую очередь распространяют среди них соответствующую идеологию. Во многом этому способствуют различные социальные сети и иные цифровые площадки, которые в последние годы стремительно развиваются, и являются средой, способной быстро распространить идеологию насилия и мобилизовать недовольных граждан.

В современных условиях цифровая среда удобна для выражения криминальной речевой агрессии и вирусоподобного, массированного распространения радикально-пропагандистской информации [3. С. 179–193]. Именно поэтому специалисты по безопасности предупреждают, что Интернет стал неконтролируемым пространством [22. Р. 57–75].

Вербовщики подтверждают, что новостные репортажи, иллюстрирующие агрессию Запада против ислама, являются особенно эффективным инструментом для привлечения внимания потенциальных членов [17. Р. 25–56] террористических, экстремистских и диверсионных формирований.

Такие платформы социальных сетей как Facebook¹, Twitter² и YouTube³, служат не только для распространения фейковых новостей, но и подстрекательства к терроризму, экстремизму, диверсии. Эти социальные сети позволяют террористическим формированиям продвигать цели движения, поддерживая коллективные онлайн-мероприятия и распространяя экстремистский насильственный контент. Практика показывает, что цифровые площадки могут оказать пагубное влияние на радикальное восприятие и поведение людей, особенно в молодом возрасте, поскольку средства массовой информации формируют способ восприятия реальности. Это приводит к искаженному восприятию реальности среди молодежи, потере доверия, а также к чувству незащищенности и неопределенности [21. Р. 995–1019].

Констатируется факт того, что, например, Аль-Каида⁴ через различные веб-сайты запускает аудио- и видеопотоки, создает форумы, онлайн-чаты, загружает листовки, распространяет средства психологического воздействия. Видео-записи атак смертников часто загружаются на цифровых площадках и широко распространяются, чтобы показать мужество террористов, их мастерство

¹ Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

² Социальная сеть заблокирована на территории Российской Федерации за распространение незаконной информации.

³ Иностранное лицо, владеющее информационным ресурсом YouTube, является нарушителем законодательства Российской Федерации

⁴ Решением Верховного Суда Российской Федерации от 14.02.2003 организация признана террористической, ее деятельность запрещена на территории Российской Федерации.

в уничтожении превосходящих по вооружению врагов. Примечательно и то, что материалы по онлайн-вербовке часто переводятся на разные языки [17. Р. 25–56].

Механизм вовлечения (склонения, вербовки) лиц в террористические, экстремистские и диверсионные преступления с использованием ИТТ. Механизм вовлечения людей в совершение террористических, экстремистских и диверсионных преступлений достаточно сложен и заключается в серьезном психологическом воздействии на человека. Это обусловлено невозможностью в одночасье превратить обычных людей в террористов, экстремистов и диверсантов. Для этого используются различные методы социального влияния.

Так, первая стадия процесса вовлечения в террористическую, экстремистскую и диверсионную деятельность нередко начинается с обычного любопытства. Лицо заходит на террористический веб-сайт, знакомится со взглядами формирования. О таких веб-сайтах люди узнают от друзей или семьи, или их приглашает посетить эти страницы кто-то, с кем они недавно познакомились [17. Р. 25–56], что вполне объяснимо.

Исследования показывают, что радикализация чаще всего происходит именно через социальные взаимодействия. Многие люди, которые присоединяются к террористическим, экстремистским или диверсионным формированиям, имеют существующие отношения с лицами, уже вовлеченными в сеть [16. Р. 491–508]. При этом здесь возможны различные типы связей (например, дружеские, родственные, служебные).

Для вербовки членов террористических, экстремистских и диверсантских формирований, а также вовлечения лиц в совершение противоправных деяний используется, в частности, метод анализа социальных сетей – «это аналитический подход, который фокусируется на субъектах социальных групп и их связях» [16. Р. 491–508]. Кроме того, большинство людей пользуются поисковыми системами в сети «Интернет» или переходят по заинтересовавшим их ссылкам. Сайты же, в свою очередь, работают обычно через технологии искусственного интеллекта, которые анализируют алгоритмы действий пользователя и собирают данные о нем.

В частности, алгоритмы поисковой рекламы Google (технология AdWord) и видеоплатформа YouTube⁵ используются для выявления тех, кто ищет контент насильственного экстремизма в Google. Эмпирические исследования, в свою очередь, показывают, что к факторам риска на индивидуальном уровне при вовлечении лица в совершение террористических, экстремистских и диверсионных преступлений большую роль играют социально-демографические характеристики такого лица, криминальное прошлое, его образование, отношение к религии, наличие работы, доход, психическое здоровье, установки и убеждения [20. Р. 1417–1435]. Все это позволяет выявить интересы такого лица, продемонстрировать ему соответствующий контент, что в последующем может быть использовано для психологического воздействия на него.

⁵ Иностранное лицо, владеющее информационным ресурсом YouTube, является нарушителем законодательства Российской Федерации

Для вербовки характерны такие способы воздействия, которые вызывают прежде всего психологическую зависимость, когда индивидуальные принципы и ценности заменяются чужими установками и программами действий. Вербовщиками активно используется технология «манипулирования», т. е. эксплуатация одного человека другим [5. С. 141–150].

Далее поступают простые, на первый взгляд безобидные онлайн-просьбы. Вербовщики действуют так, чтобы не отпугнуть потенциальных членов (для этого нельзя быть слишком настойчивым в начальном этапе контакта). Используя тактику постепенного влияния, типичный веб-сайт для онлайн-вербовки, иллюстрирует насильственные действия в небольшом объеме. На сайте представляется базовая история соответствующего движения, дается информация о его общей миссии и целях, общее описание самых значимых побед, биография почетных членов, критика противников и последние новости. По прошествии же времени от человека начинают требовать все большей приверженности делу [17. Р. 25–56].

На следующем этапе, когда лицо уже проявляет желание присоединиться к формированию, ему дается доступ к более экстремальным материалам (видео и иным медиа) [17. Р. 25–56].

У отдельных завербованных лиц есть желание стать частью группы и установить связи с иными членами формирования, так как приверженность к нему обеспечивает быструю выгоду для социальной идентичности человека как члена группы, защиту от возможности быть представленным как часть враждебной внешней группы и долгосрочную религиозную выгоду в виде духовного удовлетворения и небесных наград [17. Р. 25–56].

Вместе с тем многие люди изначально становятся вовлеченными в террористические/экстремистские/диверсионные группы по личным или социальным причинам [16. Р. 491–508]. Данная группа людей чаще всего становится так называемыми террористами-одиночками, экстремистами-одиночками или диверсантами-одиночками, но при этом их радикализация происходит, как правило, через цифровое пространство.

Более того, эмпирические исследования показывают, что одиночки более склонны обучаться онлайн (по подсчетам ученых в 2,64 раза), чем террористы, работающие в группах [15].

Социальные сети и иные цифровые площадки способствуют саморадикализации людей, предоставляя возможности получения более актуальной информации на тематических форумах и в социальных сетях. А организованные террористические/экстремистские/диверсионные группы ищут радикализированных лиц, поскольку их можно завербовать, обучить и отправить на выполнение заданий за относительно небольшие деньги [18. Р. 385–418].

Термин «одиночка» относится к лицам, которые действуют индивидуально и не являются частью соответствующей организации. Они не находятся под прямым влиянием иерархической или организационной системы, а их тактические методы, планирование и действия задуманы без прямого командования и контроля. Кроме того, акты одиночек могут быть вдохновлены идеологией или действиями организации [11. Р. 995–1019]. Специалисты также отмечают, что одиночки зачастую действуют «от имени группы, поскольку они воображают се-

бя одним из ее членов», и что «одиночки не требуют особого объяснения своего насилия» [15. Р. 491–508].

Кроме того, в научной литературе описываются ИТТ, обеспечивающие бесконтактное (дистанционное) управление не только отдельными лицами, но и толпой, в целях привлечения к рассматриваемым деструктивным действиям. Такие технологии используются при организации коллективных акций «умной толпы» для совершения террористических, экстремистских и диверсионных действий [7].

Примечательно, что «умная толпа» формируется в результате длительного диалога. Версии «умной толпы» существовали всегда (например, некоторые интеллектуалы делились различными идеями через письма, журналы и т. д.). Однако открытый и интерактивный характер цифровых площадок позволил некоторым террористическим/экстремистским/диверсионным формированиям призвать других в сообщества, которые поддерживают неприятные установки, включая идеологию насилия, дискриминационные убеждения о расе, национальности и пр. Эти крайние взгляды усиливаются в социальных сетях, а затем распространяются среди географически разбросанных участников, чтобы выйти на поверхность [19. Р. 572–577] путем совершения актов насилия, диверсий и пр.

Наиболее распространенная форма «умной толпы» – флэшмоб – организованная заранее (в том числе через интернет-пространство) массовая акция, когда большая группа лиц внезапно появляется в общественном месте и в несколько минут выполняет оговоренные заранее действия (сценарий), и быстро расходится [8. С. 53].

Так, в 2006 г. М. в составе группы лиц организовал преступное сообщество «Северное братство» для совершения экстремистских преступлений. Группа преследовала цель прихода к власти в России неконституционным путем, изменения конституционного строя и территориальной целостности государства. Для достижения этих задач был создан сайт, на котором размещались статьи об идеологии сообщества. В 2007 г. руководители группы создали интернет-проект, по правилам которого зарегистрированные участники исполняли размещенные на сайте задания экстремистской направленности [6].

Деятельность террористов/экстремистов/диверсантов-одиночек выгодна преступным формированиям, так как их атаки не такие сложные и финансово не затратные, но вызывают трудности в обнаружении и предотвращении деструктивных действий.

Вовлечение несовершеннолетних в совершение террористических, экстремистских и диверсионных преступлений с использованием ИТТ. Дело в том, что в специальных составах преступлений (ч. 1, 1¹ ст. 205¹, ч. 1 ст. 281¹, ч. 1¹ ст. 282¹, ч. 1¹ ст. 282² УК РФ) не регламентирован признак их совершения в отношении несовершеннолетних, который отягчал бы содеянное. Поэтому в случае вовлечения несовершеннолетних в совершение хотя бы одного из террористических преступлений, диверсии или в деятельность экстремистского сообщества (организации), содеянное квалифицируется по совокупности с преступлением, предусмотренным в ч. 4 ст. 150 УК РФ (вовлечение несовершеннолетнего в преступную группу). Но в ст. 150 УК РФ не зафиксирован отягчающий

признак совершение преступления с использованием ИТС, в том числе сети «Интернет».

Такая квалификация (по совокупности преступлений) обусловлена и тем, что вовлечение несовершеннолетних в преступную деятельность посягает на их нормальное нравственное и социальное развитие.

Отметим, что некоторые зарубежные страны уже внесли соответствующие изменения в национальное уголовное законодательство.

Так, ч. 2 ст. 132 УК Республики Казахстан [11] установлена ответственность за вовлечение несовершеннолетнего в совершение уголовных правонарушений посредством использования сетей телекоммуникаций, в том числе сети Интернет. Примечательно и то, что норма о вербовке или подготовке либо вооружении лиц в целях организации террористической либо экстремистской деятельности (ст. 259 УК Республики Казахстан) предусматривает в части 2 квалифицирующий признак – совершение этого деяния в отношении несовершеннолетнего. В соответствии с УК Туркменистана [14] привлечение несовершеннолетнего лица влечет повышенную ответственность при организации экстремистской организации (ч. 2 ст. 190) или привлечении лица и его подготовке к террористической и экстремистской деятельности (ч. 2 ст. 297). Законодатель Молдовы [12] установил, что вовлечение несовершеннолетнего в совершение преступления террористического характера является самостоятельным квалифицирующим признаком в норме о вовлечении таких лиц в преступную деятельность.

Заключение. Использование ИТТ при совершении названных деяний происходит в процессе выполнения их объективной стороны и обладает повышенной общественной опасностью по сравнению с аналогичными деяниями, совершаемыми офлайн. Данные деяния являются относительно распространенными, т. е. типичными, а не случайными или редкими, о чем свидетельствуют статистические данные.

Этот же признак следует предусмотреть и в составе преступления о вовлечении несовершеннолетнего в совершение преступления.

Полагаем, что введение такого признака позволит усилить меры по обеспечению информационной безопасности населения, в том числе несовершеннолетних и защиты их от информационно-психологического воздействия, пропаганды идеологии терроризма и экстремизма.

Список литературы

1. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>
2. Антонова Е. Ю. Терроризм как идеология насилия // Вестник Дальневосточного юридического института МВД России. – 2018. – № 2(43). – С. 69–74.
3. Никишин В. Д., Галяшина Е. И. Юрико-лингвистический подход к исследованию поликодовых текстов криминогенной коммуникации в цифровой среде в целях обеспечения информационной (мировоззренческой) безопасности // Актуальные проблемы российского права. – 2020. – № 6. – С. 179–193.
4. Обзор практики рассмотрения военными судами дел о преступлениях, совершение которых сопряжено с осуществлением террористической и экстре-

мистской деятельности за 2015 год / Верховный Суд Российской Федерации; Судебная коллегия по делам военнослужащих. М., 2016.

5. Палий В. В. Уголовно-правовые аспекты защиты прав несовершеннолетних от вовлечения в деструктивные группы и влияния деструктивного контента // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2024. – № 4. С. 141–150. – DOI: 10.17803/2311-5998.2024.116.4.141-150.

6. Создатель интернет-проекта «Большая Игра. Сломай Систему» за планы «бархатной» революции в РФ осужден на 9 лет // Право.ru. – URL: <https://pravo.ru/news/view/61736/> (дата обращения: 10.07.2024).

7. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.

8. Сундиев И. Ю., Смирнов А. А., Андрюхин Н. Г. Бесструктурные и бесконтактные способы вовлечения молодежи в террористическую и экстремистскую деятельность // Научный портал МВД России. – 2018. – № 2. – С. 52–60.

9. Томский областной суд вынес приговор диверсанту // Томский областной суд: [сайт]. – URL: https://oblsud.tms.sudrf.ru/modules.php?name=press_dep&op=1&did=1157 (дата обращения: 04.07.2024).

10. Уголовный кодекс Республики Армения от 05.05.2021 (по сост. на 12.04.2024). – URL: <http://www.parliament.am/legislation.php?sel=show&ID=7645&lang=rus> (дата обращения: 05.07.2024).

11. Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V (с изм. и доп. по сост. на 20.06.2024) // ИС Параграф. – URL: https://online.zakon.kz/Document/?doc_id=31575252&doc_id2=31575252#pos=138;-100&pos2=2313;-98 (дата обращения: 05.07.2024).

12. Уголовный кодекс Республики Молдова от 18.04.2002 № 985-XV (с изм. и доп. по сост. на 24.11.2023) // ИС Параграф. – URL: https://online.zakon.kz/document/?doc_id=30394923&doc_id2=30394923#activate_doc=2&pos=295;-98&pos2=2710;-126 (дата обращения: 15.07.2024).

13. Уголовный кодекс Республики Таджикистан от 21.05.1998 № 574 (с изм. и доп. по сост. на 20.06.2024) // ИС Континент. – URL: https://continent-online.com/Document/?doc_id=30397325#pos=1562;32 (дата обращения: 05.07.2024).

14. Уголовный кодекс Туркменистана от 12.06.1997 № 222-I (с изм. и доп. по сост. на 25.11.2023) // ИС Параграф. – URL: https://online.zakon.kz/Document/?doc_id=31295286&doc_id2=31295286#pos=172;-94&pos2=1560;-98 (дата обращения: 05.07.2024).

15. Binder J. F, Kenyon J. Terrorism and The Internet: How Dangerous Is Online Radicalization? // Front Psychol. – 2022 – Vol. 13:997390. – DOI: 10.3389/fpsyg.2022.997390.

16. Bright D., Whelan C., Harris-Hogan S. Exploring the hidden social networks of ‘lone actor’ terrorists // Crime, Law and Social Change. – 2020. – Т. 74. – С. 491–508.

17. Guadagno R., Lankford A., Muscanell N., Okdie B., McCallum D. Social Influence in the online Recruitment of terrorists and terrorist Sympathizers: Implica-

tions for Social Psychology Research // *Revue internationale de psychologie sociale*. – 2010. – Vol. 23. – P. 25–56.

18. Khokhlov N., Korotayev A. Internet, Political Regime and Terrorism: A Quantitative Analysis // *Cross-Cultural Research*. – 2022. – Vol. 56(4). – P. 385–418. – DOI: 10.1177/10693971221085343.

19. Relph E. Digital disorientation and place // *Memory Studies*. – 2021. – Vol. 14(3). – P. 572–577. – DOI: 10.1177/17506980211010694.

20. Scrivens R., Gill P., Conway M. The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research // *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. – 2020. – P. 1417–1435.

21. Sela-Shayovitz R., Dayan H., Hasisi B. Act of Age: Minor Lone-Actor Terrorists and Their Attacks // *Crime & Delinquency*. – 2023. – Vol. 69(5). – P. 995–1019. – DOI: 10.1177/00111287221131036.

22. Zedner L. Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism // *Common Law World Review*. – 2021. – Vol. 50(1). – P. 57–75.

И. Р. Бегишев,

доктор юридических наук, доцент,

Казанский инновационный университет имени В. Г. Тимирязова

Н. Л. Денисов,

кандидат юридических наук, доцент,

ООО «Московский правовой консалтинг»

ПРОБЛЕМЫ КРИМИНОЛОГИЧЕСКОГО ИЗУЧЕНИЯ И АНАЛИЗА ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБОРОТА ЦИФРОВОЙ ВАЛЮТЫ

Аннотация. В статье рассматриваются проблемы, являющимися препятствием для изучения преступлений, совершаемых в сфере оборота цифровой валюты. Отмечается, что выявленные проблемы нуждаются в первоочередном решении для того, чтобы обеспечить надлежащее и, прежде всего, научное обеспечение противодействия указанным преступным деяниям.

Ключевые слова: цифровые технологии, криптовалюта, цифровая валюта, криминология, преступление

PROBLEMS OF CRIMINOLOGICAL STUDY AND ANALYSIS OF CRIMES IN THE SPHERE OF DIGITAL CURRENCY TURNOVER

Abstract. The article examines the problems that are an obstacle to the study of crimes committed in the sphere of digital currency turnover. It is noted that the identified problems need to be addressed as a matter of priority in order to ensure proper and, above all, scientific support for countering these criminal acts.

Keywords: digital technologies, cryptocurrency, digital currency, criminology, crime

Начиная разговор о криминологической характеристике преступлений в сфере оборота цифровой валюты, следует, прежде всего, отметить, что полу-

чить достоверные, объективные и официальные данные относительно состояния, структуры и динамики данных преступлений невозможно. Это обусловлено следующими проблемами.

Во-первых, отсутствие данных официальной статистики по преступлениям в сфере оборота цифровой валюты. Обратиться к официальным данным относительно количества криптопреступлений не представляется возможным в силу того, что в официальных данных статистики отсутствуют какие-либо сведения о таких преступлениях. Это обусловлено тем, что статистический учет преступлений осуществляется в соответствии с межведомственным нормативным правовым актом [1]. В нем приводятся формы статистических карточек, которые заполняются при возбуждении уголовных дел и принятии по ним решений. Цифровые валюты никак в данных карточках не фигурируют. Единственными ориентирами служат отражаемые способы совершения преступлений в виде использования: компьютерной техники, программных средств, машинных носителей; фиктивных электронных платежей; сети Интернет. Однако данные способы в настоящее время используются для совершения значительного количества иных преступлений, поэтому для определения истинного положения дел с рассматриваемыми преступлениями необходимо фактически изучать каждое дело. Охватить весь объем таких дел затруднительно, поэтому рассмотреть можно только ограниченное их количество, чтобы определить типичные ситуации и сформировать представление об иных обстоятельствах совершения данных преступлений.

Для решения указанной проблемы необходимо, на наш взгляд, необходимо внести изменения в указанные формуляры, включив криптовалюту как специфический предмет преступления.

Во-вторых, высокий уровень латентности преступлений, в которых фигурирует криптовалюта. Следует отметить, что значительную массу таких преступлений составляют два типа преступных деяний: хищения и (или) преступления с использованием технических средств и сети Интернет. Данные преступления сами по себе достаточно высоко латентные, однако если в них фигурирует еще и криптовалюта с ее неопределенным статусом и регулированием, то это еще больше повышает латентность таких преступлений. Для определения уровня латентности данных преступлений нами было проведено исследование методом массового опроса.

Для улучшения ситуации необходимо разработать и внедрить более эффективные методики раскрытия, повысить мотивацию сотрудников, улучшить координацию и надзор, а также обеспечить надежную статистическую базу для более точной оценки уровня преступности.

Латентность таких преступлений усугубляет проблемы с их раскрываемостью.

В-третьих, неопределенность понимания круга преступлений, которые должны охватываться криминологическими исследованиями данного феномена.

Данная дискуссия нами обозначена не на пустом месте. Дело в том, что такая проблема в настоящее время присуща, например, коррупционным преступлениям. В 2013 году вышло постановление Пленума Верховного Суда Российской Федерации [2], где был приведен широкий перечень таких преступлений.

Однако в дальнейшем в период с 2016 по 2023 год был принят ряд совместных указаний Генпрокуратуры России и МВД России [3, 4], где в Перечне № 23 круг преступных деяний коррупционной направленности расширился и корректировался. Не вдаваясь детально в суть происходящего, хотелось обозначить тот факт, что в связи с данными изменениями в подходах к пониманию указанных преступлений исследования, проводимые в отношении них в разные годы и разными изыскателями, к сожалению, утрачивают преемственность и возможность прослеживания тенденции и определения трендов в их развитии. Кроме того, что является существенной проблемой, нивелирующей все затраты в рамках данных исследований, разработки методик, методов и способов предупреждения таких преступлений. Фактически каждый год можно заниматься исследованиями и разработками проблем предупреждения коррупционных преступлений исходя из нового круга таких преступлений, официально закрепленных в соответствующих документах.

Таким образом, можно отметить, что в настоящее время имеют место три основные проблемы, которые являются препятствием для изучения преступлений, совершаемых в сфере оборота цифровой валюты: отсутствие данных официальной статистики по преступлениям в сфере оборота цифровой валюты, высокий уровень латентности данных преступлений и неопределенность понимания круга преступлений, которые должны охватываться криминологическими исследованиями данного феномена. Это не единственные проблемы, но именно они нуждаются в первоочередном решении для того, чтобы обеспечить надлежащее и, прежде всего, научное обеспечение противодействия указанным преступным деяниям.

Список литературы

1. Приказ Генеральной прокуратуры РФ, МВД РФ, МЧС РФ, Минюста РФ, ФСБ РФ, Министерства экономического развития и торговли РФ и Федеральной службы РФ по контролю за оборотом наркотиков от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений» // Российская газета. 2006. № 13.
2. Постановление Пленума Верховного Суда Российской Федерации от 09.07.2013 № 24 (ред. от 24.12.2019) «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях».
3. Указание Генеральной прокуратуры РФ и МВД России от 13.12.2016 №с797/11/2 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности».
4. Указание Генеральной прокуратуры РФ и МВД России от 19.06.2023 №С401/11/2 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности».

И. Р. Бегишев,

доктор юридических наук, доцент,

Казанский инновационный университет имени В. Г. Тимирязова

А. А. Хусаинов,

магистрант,

Казанский инновационный университет имени В. Г. Тимирязова

СОДЕРЖАНИЕ И ТЕНДЕНЦИИ ЦИФРОВОЙ ПРЕСТУПНОСТИ

Аннотация. В статье рассматриваются последствия использования преступным элементом высоких технологий в противоправных целях. Отмечается, что цифровая трансформация общества и государственного аппарата привела как к положительным последствиям, так и негативным, в частности к увеличению зафиксированных деяний, связанных с цифровыми технологиями. Указываются факторы, приводящие к низкой раскрываемости цифровых преступлений. Утверждается, что терминология цифровой преступности, в связи с более широким охватом преступной направленности, является более объемным определением, чем компьютерная преступность.

Ключевые слова: цифровые технологии, криминология, преступление, преступность, уголовное право

THE CONTENT AND TRENDS OF DIGITAL CRIME

Abstract. The article examines the consequences of the use of high technologies by a criminal element for illegal purposes. It is noted that the digital transformation of society and the state apparatus has led to both positive and negative consequences, in particular to an increase in recorded acts related to digital technologies. The factors leading to a low detection rate of digital crimes are indicated. It is argued that the terminology of digital crime, due to the wider coverage of criminal orientation, is a more voluminous definition than computer crime.

Keywords: digital technologies, criminology, crime, criminality, criminal law

Развитие и усложнение экономических взаимоотношений привело к необходимости улучшения качества человеческой жизнедеятельности. Так, в результате направленных действий, вызванных потребностью достижения экономической эффективности, наступили периоды научно-технологических преобразований. По итогу таковых изменений были созданы средства и инструменты, позволяющие упростить развитие общественных отношений. Однако такая новая формация технологических инструментов привела к негативным последствиям, когда преступные элементы начинают использовать новейшие технологии в противоправных целях.

В результате технологических трансформаций произошло усиление интеграционных процессов развития цифровой среды и общества, как на региональном, так и общемировом пространстве. Именно в данном периоде были созданы сети, системы, а также устройства, которые обладают достаточно значительным цифровым потенциалом. Однако любая деятельность, которая предполагает развитие цифровых технологий, приводит к двояким последствиям, когда увеличи-

вается количество совершенных и выявленных преступлений в рассматриваемой сфере.

Так, согласно статистическим мировым данным, на 2023 г., в процентном соотношении из 8 млрд проживающих на Земле лиц, 64,4 %, что составляет порядка 5,16 млрд людей, имеют доступ и пользуются Всемирной паутиной. При этом из указанной социальной группы порядка 4,76 млрд человек являются пользователями социальных сетей [2].

Цифровая трансформация общества и государственного аппарата привела как к положительным последствиям, так и негативным, в частности к увеличению зафиксированных деяний, связанных с цифровыми технологиями. Так, в период с 2014 г. по 2023 г. произошел рекордный рост, в процентном соотношении, данной группы преступлений (4 746,4 %). При этом коэффициент выявления и раскрытия данной группы преступных деяний, является достаточно низким (23,4 %), что говорит об их высокой степени латентности [3].

К факторам, приводящим к низкой раскрываемости, можно отнести следующие:

- слабо регламентирована законодательная база относительно «пакета технологических законов»;
- отсутствуют необходимые методические рекомендации, регулирующие вопросы квалификации преступлений с использованием цифровых технологий;
- отсутствуют специальные познания функционально-технического характера у лиц, раскрывающих такие преступления.

Исходя из вышесказанного, мы можем предположить, что терминология цифровой преступности, в связи с более широким охватом преступной направленности является более объемным определением, чем компьютерная преступность.

На сегодняшний период, в правовых нормах, в судебных разьяснениях, а также в научной литературе, отсутствует определение словосочетания «цифровое преступление». Зачастую, преступления, совершаемые в цифровом пространстве, обозначают как компьютерные преступления, что является достаточно условным.

В качестве места совершения либо средства преступного деяния используется само онлайн-пространство. В рамках обеспечения безопасности, на уровне как национального регулирования, так и общемирового понимания, необходимо вырабатывать общие детерминанты уголовно-правового противодействия такого рода преступности [4].

Таким образом, можно заключить, что при активном внедрении в государственную систему цифровых технологий общество будет нуждаться в разработке государственной политики, решающей следующие задачи:

- обеспечение безопасности личности, общества и государства в цифровой сфере;
- противодействие преступлениям в цифровой сфере.

Список литературы

1. IoT, Big Data, AI, блокчейн и цифровые платформы: какие технологии изменят мир поставок. URL: <https://rg.ru>

2. Digital 2023: Global Overview Report. URL: <https://datareportal.com>

3. Пинкевич Т. В. Уголовно-правовой и криминологический понятийный аппарат в условиях цифровизации: проблемы применения // Уголовное законодательство: вчера, сегодня, завтра: материалы ежегодной Международной научно-практической конференции, Санкт-Петербург, 09–10 июня 2023 года. Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2023. С. 214–219. EDN NYCPZY.

4. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения. 2-е изд. Москва: Издательский Дом «Инфра-М», 2022. 351 с. EDN MPWWHL.

А. В. Вальтер,
старший преподаватель,
Тюменский институт повышения квалификации
сотрудников МВД России
Д. Ю. Гончаров,
доктор юридических наук, профессор,
Тюменский институт повышения квалификации
сотрудников МВД России

ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ ДЛЯ ЭВМ «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ПРОТИВОДЕЙСТВИЯ НАЛОГОВЫМ ПРЕСТУПЛЕНИЯМ» И ПЕРСПЕКТИВЫ ЕЕ ПРИМЕНЕНИЯ

Аннотация. В работе приведены примеры использования программы для ЭВМ «Искусственный интеллект противодействия налоговым преступлениям», очерчены перспективы ее применения для автоматической квалификации и прогнозирования имеющихся признаков составов преступлений, предусмотренных ст. 198–199 УК РФ.

Ключевые слова: искусственный интеллект по налоговым преступлениям, нейронная сеть, цифровые технологии, автоматизированная квалификация по ст. 198–199 УК РФ

EXAMPLES OF USING THE COMPUTER PROGRAM "ARTIFICIAL INTELLIGENCE FOR COUNTERING TAX CRIMES" AND THE PROSPECTS FOR ITS APPLICATION

Abstract. The paper provides examples of using the computer program "Artificial intelligence for countering tax crimes", outlines the prospects for its application for automatic qualification and forecasting of existing signs of crimes provided for in Articles 198-199 of the Criminal Code of the Russian Federation.

Keywords: artificial intelligence for tax crimes, neural network, digital technologies, automated qualification under Articles 198-199 of the Criminal Code of the Russian Federation.

Программа для ЭВМ «Искусственный интеллект противодействия налоговым преступлениям», может стать неоценимым инструментом для должностных лиц правоохранительных органов при квалификации материалов проверки и прогнозе по налоговым преступлениям [1–3]. Используя программу, указанные должностные лица смогут анализировать сложные бланкетные схемы по неуплате налогов в крупном и особо крупном размере, в том числе давать предварительную оценку групповым преступлениям по ст. 198–199 УК РФ [6]. Программа с учетом ее потенциала способна выявлять сложные схемы финансовых операций и транзакций, целью которых может являться преступный уход от налогообложения. Программа ЭВМ упрощает задачу правоохранительных органов по сбору доказательств и их систематизации.

Также программа может быть использована в ходе проведения налоговых экспертиз [4, 5] по исследованию исполнения обязательств по исчислению налогов и сборов, экономических судебных экспертиз и т. д. по ст. 198–199 УК РФ, т. е. возможно дальнейшее внедрение соответствующей методики при проведении судебных экспертиз по налоговым преступлениям, с учетом дальнейшего анализа и обновления программы.

Сокращение времени на расследование уголовного дела – автоматизация анализа внесенных в программу данных позволит в будущем значительно сократить время, затрачиваемое на проведение расследований по налоговым преступлениям. Программа может достаточно быстро обрабатывать большие объемы данных, вбирая ключевые моменты для квалификации и прогноза с учетом «семантического ядра». В дальнейшем, в ходе дообучения и обновления программы, будут даваться определенные рекомендации по недостающим признакам объективной и субъективной стороны по ст. 198–199 УК РФ (система обратной связи).

Перспективы повышения точности по квалификации преступлений и обратной связи с оператором программы (пользователем) – система предоставляет рекомендации по квалификации действий субъектов на основе анализа текстов дел и «семантического ядра», что повышает точность квалификации преступлений и уменьшает вероятность ошибок в ходе предварительного анализа материала. В будущем возможно закрепление на законодательном уровне вопросов машиночитаемого анализа и прогноза, с учетом внедрения, апробации, дообучения и обновления программы по налоговым преступлениям «Искусственный интеллект противодействия налоговым преступлениям».

Перспективы использования программы ЭВМ по автоматической генерации отчетов – в ближайшем будущем программа сможет генерировать отчеты относительно проведенного анализа представленного материала по ст.ст. 198–199 УК РФ, что также упростит процесс сбора доказательств, проведения следственных действий и иных документов для дальнейшего расследования или судебного разбирательства по налоговым преступлениям.

Юридические фирмы и предприниматели также смогут анализировать определенные данные в системе и получать прогнозируемые результаты, что поможет им спроектировать налоговую политику организаций, правильно оптимизировать систему налогообложения с целью минимизации рисков по возможному привлечению к уголовной ответственности.

Представители ФНС РФ могут использовать программу ЭВМ в ходе проведения мер налогового контроля с учетом имеющихся предварительных данных по ст. 198–199 УК РФ, что позволит сократить время по сбору доказательственной базы объективных и субъективных признаков состава налоговых преступлений в ходе проведения выездных и камеральных налоговых проверок и повысить качество собранного материала до передачи в правоохранительные органы.

В будущем программа ЭВМ будет дополнена новыми функциями и возможностями, включая: интеграцию с внешними системами и базами данных, на примере баз данных судебных решений РФ, а также предоставление соответствующих уголовно-правовых и иных рекомендации в ходе планирования и проведения следственных действий по налоговым преступлениям с учетом способов неуплаты налогов, сборов и страховых взносов.

Анализ больших данных: внедрение методов анализа больших данных для обработки огромных объемов информации, с учетом расширения функционала. Возможное внедрение в мобильные приложения, для оперативного доступа оператора к системе с мобильных устройств: планшетов, мобильных устройств и т. д. Авторами планируется расширение функционала путем добавления новых функций для анализа иных налоговых преступлений, связанных с неисполнением обязанности налогового агента (ст. 199.1 УК РФ), сокрытием денежных средств либо имущества организации или индивидуального предпринимателя, за счет которых должно производиться взыскание налогов, сборов, страховых взносов (ст. 199.2 УК РФ), а также уклонение страхователя – физического лица или организации – от уплаты страховых взносов на обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний в государственный внебюджетный фонд (ст. 199.3 и ст. 199.4 УК РФ).

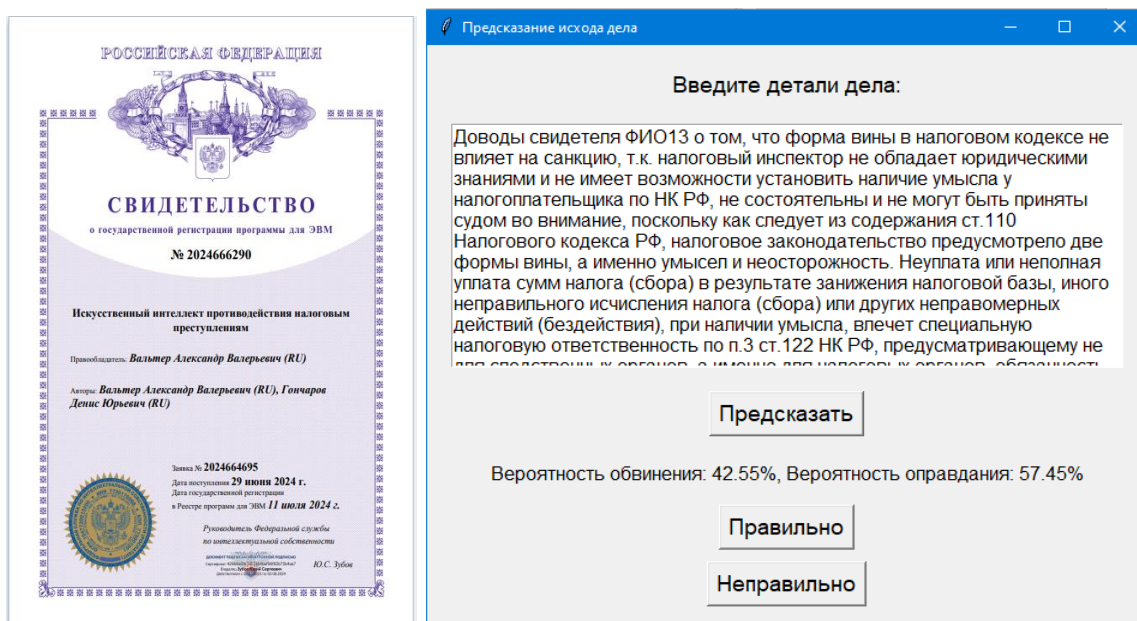


Рис. 1. Свидетельство и регистрации и интерфейс программы для ЭВМ «Искусственный интеллект противодействия налоговым преступлениям»

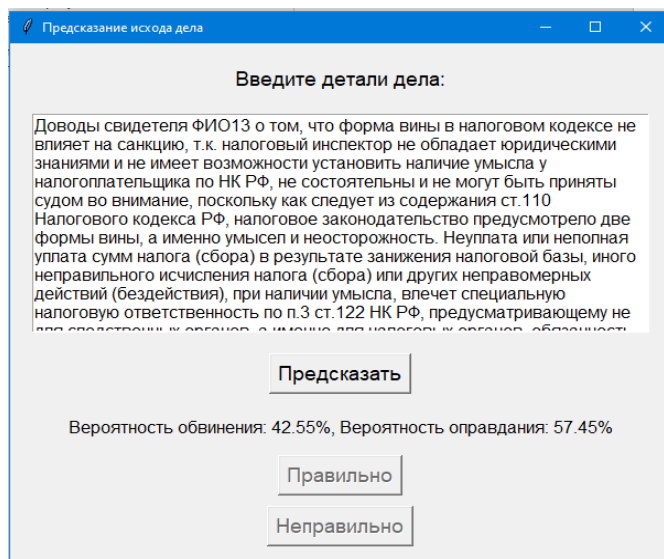


Рис. 2. Интерфейс программы для ЭВМ – «Искусственный интеллект противодействия налоговым преступлениям»

Вклад авторов в изобретение (создание программы ЭВМ)

Разработка программы ЭВМ «Искусственный интеллект противодействия налоговым преступлениям» осуществлялась в соавторстве. Авторы программы ЭВМ: Вальтер Александр Валерьевич и Гончаров Денис Юрьевич.

Личный вклад Вальтера А. В. в изобретение в ходе создания программы ЭВМ, включает:

1. Проектирование графического интерфейса для пользователя (GUI): разработку интерфейса для ввода данных, отображения результатов и ввода обратной связи в виде кнопок «предсказать», «правильно» и «неправильно».

2. Идею и концепцию по созданию программы ЭВМ «Налоговый интеллект по ст. 198–199 УК РФ» по автоматизированному анализу признаков состава налогового преступления, подбор соответствующего языка программирования «Python» [6].

3. Проектирование, анализ и разработка «семантического ядра» по ст.ст. 198, 199 УК РФ: Создание и внедрение семантического ядра, включающего исследование судебной практики по ст.ст. 198–199 УК РФ, налогового законодательства РФ, ст.ст. 198, 199 УК РФ, и выделения соответствующих ключевых фраз для элементов «обвинения» и «оправдания».

4. Анализ и проектирование данных: основную работу по анализу данных и приисканию подходящих алгоритмов для обучения программы ЭВМ.

5. Интеграцию библиотек в программу ЭВМ: выбор и интеграцию основных библиотек для обработки естественного языка и машинного обучения.

6. Поиск и разработку концепции обучения и дообучение модели относительно изначальных целей и задач программы ЭВМ.

7. Проектирование механизма обратной связи и дообучения: разработку и внедрение механизмов сбора и обработки обратной связи программы ЭВМ.

Личный вклад Д. Ю. Гончарова в ходе создания программы ЭВМ, включает следующие компоненты:

1. Тестирование программы: проведение тестирования и предоставление рекомендаций по работе программы для выявления и устранения ошибок, а также для улучшения производительности и надежности системы.

2. Профессиональное консультирование по доктринальным вопросам уголовного права в части объективных и субъективных признаков состава преступления [6] в ходе проектирования программы ЭВМ.

Список литературы

1. Вальтер А. В. Вопросы бланкетности, семантики и скрытой налоговой преюдиции по уголовно-правовым нормам, предусмотренным ст.ст. 198–199.4 УК РФ // Вестник Восточно-Сибирского института МВД России. 2023. № 4(107). С. 112–125.

2. Вальтер А. В. Семантический анализ терминологии в нормах, предусмотренных ст. ст. 198–199.4 УК РФ: кибернетический подход // Вопросы российской юстиции. 2024. № 31. С. 257–265.

3. Гончаров Д. Ю. Семантические особенности норм о налоговых преступлениях и некоторые вопросы их толкования // Правопорядок: история, теория, практика. 2024. №3 (42).

4. Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ (ред. от 08.08.2024) (с изм. и доп., вступ. в силу с 12.08.2024) // Собрание законодательства РФ. 07.08.2000. № 32, ст. 3340.

5. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ (ред. от 08.08.2024) // Российская газета. 1998. № 148–149. 06 авг.

6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. 1996. № 25, ст. 2954.

Е. Л. Власова,

доцент,

Саратовский национальный исследовательский
государственный университет имени Н. Г. Чернышевского

А. Д. Глезова,

студент,

Саратовский национальный исследовательский
государственный университет имени Н. Г. Чернышевского

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ КАК ОСНОВНАЯ ПРОБЛЕМА В СОВРЕМЕННОМ ОБЩЕСТВЕ

Аннотация. В данной статье определены главные проблемы, связанные с предупреждением преступлений, совершаемых с использованием информационных технологий. В настоящее время, виртуальное пространство стало частью жизни людей, в связи с чем возникает рост киберпреступлений, оказывающий негативное воздействие на различные сферы жизнедеятельности общества.

Ключевые слова: киберпреступления, информационные технологии, цифровизация, экономическая безопасность, киберугрозы, национальная безопасность, персональные данные

COUNTERING CYBERCRIME AS A MAJOR PROBLEM IN MODERN SOCIETY

Abstract. This article identifies the main problems associated with the prevention of crimes committed using information technology. Currently, the virtual space has become a part of people's lives, and therefore, there is an increase in cyberspace, which has a negative impact on various spheres of society.

Keywords: cybercrime, information technology, digitalisation, economic security, cyber threats, national security, personal data

Введение. В настоящее время, виртуальное пространство неотъемлемо присутствует в жизни человека. Способ общения в сети Интернет с каждым годом набирает все большую популярность, так как является оптимальным и быстрым. Тем не менее существуют и отрицательные аспекты, связанные с информационной безопасностью пользователей, защитой их персональных данных от злоумышленников [3]. В связи с чем ежегодные показатели киберпреступлений по стране значительно возрастают.

Основная часть. Данный вид преступления затрагивает разнообразные сферы жизни и наносит ущерб не только личной безопасности граждан, но также экономической и национальной безопасности государства.

Вопрос по борьбе с киберпреступлениями является весьма актуальным и распространен во всем мире, так как различная информация в наше время представляет огромную ценность и является ресурсом, оказывающим влияние на все сферы жизнедеятельности общества. За последние годы в информационном пространстве увеличилось число лиц, обладающих высоким уровнем компетенции, которые входят в организованные преступные кибергруппы [8. С. 99–100]. В связи с распространением COVID-19 в России фиксируется снижение уличной преступности, но в то же время дистанционный формат работы повлиял на переход преступников в компьютерную сферу [7].

Существует ряд информационно-технических средств, с помощью которых совершаются киберпреступления. К таким средствам можно отнести:

- 1) мессенджеры;
- 2) интернет-сайты;
- 3) навигационную технику;
- 4) гаджеты;
- 5) беспилотные летательные аппараты [2. С. 151–152].

Преступления в сети Интернет являются самыми непредсказуемыми и опасными, так как вред, причиненный таким видом посягательства, имеет различные последствия.

Одним из факторов существования организованной киберпреступности является ее высокий уровень латентности, который способствует формированию мнения о возможности безнаказанного совершения преступлений.

На фоне происходящих событий в нашей стране образовались некоторые разновидности киберпреступлений, к которым можно отнести:

- 1) распространение недостоверной (ложной) информации;
- 2) неправомерный доступ, включая кибератаки на сайты государственных органов (для получения служебной информации в личных целях, а также для приостановления рабочего процесса);
- 3) мошеннические действия в банковской сфере [4. С. 36];

4) незаконный оборот запрещенных веществ через мессенджеры и т. д. [9. С. 96; 1. С. 124–128];

С каждым годом набирают популярность различные игровые платформы это связано с тем, что люди находятся в поиске новых способов развлечений и общения.

Онлайн-игры – довольно прибыльная платформа, на которой осуществляются продажи различных игровых предметов и подписок, являющихся законным платежным средством, что привлекает киберпреступников на совершение правонарушений в данной отрасли, а именно:

1) осуществление заражения устройств вредоносными файлами, которые способны следить за информацией, вводимой на клавиатуре и изымать информацию учетных данных;

2) создание фальшивых сайтов, схожих с официальными, для хищения учетных данных и денежных средств и т. д. [6. С. 175].

Согласно юридической литературе, киберпреступность составляет серьезную угрозу для граждан и государства в целом. Для снижения масштабов таких проявлений необходимо усовершенствовать не только защиту программных обеспечений, но и методы организационного и правового характера [5. С. 102].

Для улучшения противодействия киберпреступлениям предлагаем следующие меры:

1) создание специализированных курсов обучения сотрудников правоохранительных органов основам и методам борьбы с киберпреступностью;

2) внесение ужесточительных мер наказания в законодательство;

3) просвещение населения об опасности кидберпреступлений путем проведения лекций, конференций в учебных и государственных учреждениях, а также публикаций в средствах массовой информации и социальных сетях.

Также необходимо проанализировать не только отечественную, но и зарубежную судебную практику и статистику раскрываемости преступлений, что позволит более детально проработать существующие методы и создать новые, более эффективные.

Заключение. Таким образом, на основании вышеизложенного мы пришли к тому, что киберпреступность является видом преступности, включающим в себя противоправные действия, совершаемые с использованием Интернета и компьютерных технологий. В настоящее время развитие современных технологий носит как положительный, так и отрицательный характер. Рост киберпреступлений стал серьезной проблемой в современном обществе и в целях противодействия их совершения необходимо разработать методы, направленные на повышение уровня эффективности правоохранительных органов и бдительности граждан.

Список литературы

1. Власова Е. Л., Устьянцева О. В. Современные направления противодействия незаконной торговле морскими млекопитающими в Российской Федерации // Хозяйство и право. 2020. № 2 (517). С. 124–128.

2. Долженко Н. И., Ярощук И. А. Киберпреступность как одна из ключевых проблем современности // Правовая парадигма. 2020. Т. 19, № 1. С. 151–157.

3. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.
4. Зверева Е. Б. Киберпреступность как угроза безопасности современного общества: виды, особенности, методы борьбы и профилактики // Молодой ученый. 2020. № 10. С. 35–37.
5. Кобец П.Н. Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт // Научный вестник Омской академии МВД России. 2022. № 2. С. 101–105.
6. Мартьянов Н. Р. Уголовно-правовая борьба с киберпреступлениями на современном этапе // Государственная служба и кадры. 2020. № 1. С. 175–177.
7. Статистика и аналитика // Официальный сайт МВД России. URL: <https://мвд.рф> (дата обращения: 06.09.2024).
8. Тимофеев А. В., Комолов А. А. Киберпреступность как социальная угроза и объект правового регулирования // Вестник Московского государственного областного университета. Сер.: Философские науки. 2021. № 1. С. 95–101.
9. Чуманов А. С. Проблемы противодействия незаконному обороту наркотических средств, психотропных веществ или их аналогов с использованием информационно-телекоммуникационных сетей // Киберпреступность: риски и угрозы. материалы Всерос. студ. круглого науч.-практ. стола с междунар. участием (г. Санкт-Петербург, 11 февраля 2021 г.). СПб. Астерион, 2021. С. 96–99.

Э. М. Гильманов,
старший преподаватель,
Казанский инновационный университет
имени В. Г. Тимирязова,
А. М. Бабаева,
студент,
Казанский инновационный университет
имени В. Г. Тимирязова

ИСПОЛЬЗОВАНИЕ КРИМИНАЛИСТИЧЕСКИХ МЕТОДИК ДЛЯ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В ЦИФРОВОЙ СФЕРЕ

Аннотация. В связи с цифровым развитием общества криминалистика тоже должна идти в ногу со временем и применять более современные инструменты и методики как для разработки, так и применения научных достижений во имя предотвращения нетривиальных преступлений, доселе невиданных.

Ключевые слова: искусственный интеллект, криминалистика, методы, преступление, цифровизация, киберпреступность, расследование

THE USE OF FORENSIC TECHNIQUES TO SOLVE CRIMES IN THE DIGITAL SPHERE

Abstract. Due to the trends in the development of society as a whole, criminology must keep up and apply more and more modern tools and techniques both

for the development and application of scientific achievements in the name of preventing non-trivial crimes hitherto unseen.

Keywords: artificial intelligence, criminology, methods, crime, digitalization, cybercrime, investigation

Введение. В соответствии с современными положениями российского законодательства о развитии искусственного интеллекта, это технология, позволяющая использовать мощности компьютерного устройства для анализа большого объема данных. И это, в силу его природы, превосходит скорость и качество работы, обусловленные отсутствием эмоций (человеческого фактора).

Перспектива синтеза искусственного интеллекта с работой органов предварительного следствия и разработкой новых методик представляется весьма успешной в силу титанических размеров баз данных, применяемых в ходе уголовного судопроизводства. Ведь, как известно, разнообразие способов совершения преступлений в цифровой сфере оставляет за собой и обуславливает возникновение цифровых следов [2. С. 130].

Основная часть. Как и у каждой группы преступлений, у киберпреступлений есть своя специфика. Ей являются многочисленные и разноплановые инструменты, используемые при их осуществлении. В этой связи уникальная правовая природа киберпреступлений определяет и особенности криминалистических методов по противодействию им [1. С. 170–171].

С одной стороны, криминалистические методы борьбы имеют свои подходы к толкованию киберпреступлений: большой объем информационных данных, потенциально обладающий признаками противообщественной направленности. Стоит отметить, что из всех настолько проработанная возможность совершения деяния при помощи компьютерных технологий обозначена только при мошенничестве [3. С. 36].

Так называемая компьютерная криминалистика, исходя из названия, предполагает использование в ходе расследования навыков по использованию цифровых и технологических достижений науки. Это будет способствовать разработке новых методов по сбору, анализу, сохранению и регистрации доказательств. Например, после получения результатов судебной экспертизы, следователи по борьбе с киберпреступностью связываются с компаниями, обеспечивающими подключение к информационно-телекоммуникационным сетям. Это происходит с целью выяснения, какие ресурсы или протоколы подключения использовались для совершения преступления [4. С. 30–31; 5. С. 650–668].

Еще не до конца изученными являются возможности искусственного интеллекта к самообучению: его пределы, скоростные лимиты, количество используемого трафика (данный вопрос создает дополнительный мотив к призыву компаний, обеспечивающих соединение искусственного интеллекта с информационно-телекоммуникационной сетью «Интернет» к сотрудничеству с органами уголовного розыска), что напрямую коррелирует с потенциальными возможностями методологии и инструментария криминалистики по отношению к расследованию киберпреступлений. Многими авторами исследуются вопросы принципов технологии искусственного интеллекта для успешного и эффективного его применения [6], что можно также весьма положительно оценить.

Заключение. Подводя итог, основополагающим отличием киберпреступлений является применение компьютеров в качестве «орудия» преступления. Соответственно, и методы криминалистической борьбы и противодействие им должны быть обеспечены новейшими достижениями компьютерной техники.

В частности, самым базовым применением искусственного интеллекта в борьбе с киберпреступлениями может послужить в качестве инструмента более качественный анализ данных по определенной категории преступлений (например, преступлений против половой свободы и половой неприкосновенности или преступления против экономики), включая запись камер видеонаблюдения, точные координаты места совершения преступления и т. д. Однако это упирается в нарушение конституционных прав и свобод человека и гражданина в плане сбора и применения личных данных преступника.

Список литературы

1. Болтенкова Ю. В. Особенности расследования преступлений, совершаемых с использованием IT-технологий в сфере компьютерной информации // Поколение будущего: Взгляд молодых ученых – 2022: сборник научных статей 11-й Международной молодежной научной конференции, Курск, 10–11 ноября 2022 года. Том 2. – Курск: Юго-Западный государственный университет, 2022. – С 170–174. – EDN YZQBVM.
2. Климова Я. А. Цифровая криминалистика: перспективы развития // Вестник Волгоградской академии МВД России. 2020. №4 (55). URL: <https://cyberleninka.ru/article/n/tsifrovaya-kriminalistika-perspektivy-razvitiya>
3. Сарычев А. В., Архипцев И. Н. Современное состояние раскрытия и расследования преступлений, совершаемых с использованием информационных технологий // ППД. 2020. № 1. URL: <https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-raskrytiya-i-rassledovaniya-prestupleniy-sovershaemyh-s-ispolzovaniem-informatsionnyh-tehnologiy>
4. Шевченко Е. С. О криминалистической трактовке понятия «киберпреступность» // Информационное право. 2014. № 3. С. 29–32. EDN SHOSCH.
5. Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности / Е. А. Русскевич // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650–672. EDN FISEET.
6. Харитонов Ю. С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // Journal of Digital Technologies and Law. 2023. № 1(2). С. 337–358. EDN: dxnwhv

Э. М. Гильманов,
старший преподаватель
Казанский инновационный университет имени В. Г. Тимирязова,
Р. Э. Гильманов,
магистрант,
Казанский инновационный университет имени В. Г. Тимирязова,
Э. Е. Азаров,
студент,
Казанский инновационный университет имени В. Г. Тимирязова

ОТВЕТСТВЕННОСТЬ ЗА РАСКРЫТИЕ ПОСРЕДСТВОМ СЕТИ ИНТЕРНЕТ ДАННЫХ, СТАВШИХ ИЗВЕСТНЫМИ В ХОДЕ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Аннотация. Широкую известность в настоящее время приобретает использование сети Интернет при раскрытии и расследовании преступлений, а также в процессе коммуникации между участниками уголовного процесса и иными заинтересованными лицами. Следовательно возрастает вероятность случайно или преднамеренно раскрыть конфиденциальную информацию и сделать ее достоянием общественности. Это может существенно затруднить расследование или облегчить сокрытие следов преступления, либо предупредит вероятного преступника о том, что в отношении него проводятся следственные мероприятия, и, соответственно, за утечку данной информации обязательно требуется установление ответственности. Данная научная работа посвящена анализу возможных мер ответственности за раскрытие данных, выявленных в ходе следственных мероприятий, через сеть Интернет.

Ключевые слова: информационные технологии, сеть Интернет, информация, подлежащая раскрытию, следственные действия, уголовное судопроизводство

RESPONSIBILITY FOR THE DISCLOSURE VIA THE INTERNET OF DATA THAT BECAME KNOWN DURING THE COURSE OF INVESTIGATIVE ACTIONS

Abstract. The use of the Internet in the detection and investigation of crimes, as well as in the process of communication between participants in criminal proceedings and other interested persons, is currently becoming widely known. However, as a result of such interaction, there is a high probability that information that is confidential or relevant to a preliminary investigation or investigative actions may be accidentally or intentionally disclosed and become public. However, this can significantly complicate the investigation or facilitate the concealment of traces of a crime, or it will warn the likely perpetrator that investigative measures are being carried out against him, and, accordingly, responsibility must be established for the leakage of this information. This scientific work is devoted to the analysis of possible measures of responsibility for the disclosure of data identified during investigative activities via the Internet.

Keywords: information technology, Internet, information to be disclosed, investigative actions, criminal proceedings

Уголовный процесс и криминалистика в настоящее время сталкиваются с огромным потоком цифровой информации на разных этапах расследования преступлений. Стоит согласиться с мнением о том, что цифровизация оказывает колоссальное влияние на уголовное правосудие [5. С. 237]. Соответственно, возникает необходимость усовершенствования мер ответственности, которая может быть применима к указанным лицам в случае распространения указанной информации, в том числе посредством сети Интернет.

В информационно-телекоммуникационной сети «Интернет» основной перечень вопросов, по мнению законодателя, был закрыт, а впоследствии четко определен посредством их приведения в статье 161 Уголовно-процессуального кодекса Российской Федерации. Тайна следствия включает ряд взаимосвязанных ситуаций, направленных на наиболее полное раскрытие и расследование преступления.

Нельзя не согласиться с позицией законодателя в рамках определения объема той информации, которая может подлежать дальнейшему раскрытию, но с согласия самого следователя, непосредственно отвечающего за ведение уголовного следствия, так и дознавателя. Отметим, что и сама по себе цифровая информация может стать источником формирования системы доказательств по конкретному уголовному делу [1. С. 350].

К сожалению, активное развитие социальных сетей, их стремительное распространение, массовость, включенность в мировые общественные и политические процессы, наличие практически у каждого мобильных средств связи способствуют возникновению ситуаций девиантного поведения [2], когда посторонние лица фотографируют или иным образом фиксируют место совершения преступления или сам процесс проведения следственных мероприятий (особенно если они проводятся в публичном месте), а затем выкладывают эту информацию в свободном доступе. В современных мессенджерах (например, ВКонтакте или Telegram, а также иных) создаются целые сообщества, в которых заинтересованные лица распространяют такую информацию. При этом иногда такую информацию «сливают» сами участники следственных мероприятий (обычно оставаясь в анонимном статусе). В то же время необходимо осуществлять защиту цифровых прав граждан [3] и оберегать их от преступных посягательств.

Также нужно учитывать, что определенную специфику имеют уголовно-процессуальные действия, совершаемые в отношении иностранных граждан, особенно обладающих дипломатическим или иным иммунитетом [4. С. 368], информация о которых распространению не подлежит.

Как нам видится, в рамках статьи 161 УПК РФ не отражены необходимые положения о подчиненности указанных лиц в рамках организации структуры государственных органов, осуществляющих расследование уголовных дел, ввиду того что основные следственные действия осуществляются следователем, дознавателем с позиции согласования данных действий с руководителем следственного органа, исходя из перечисленных полномочий в рамках статьи 39 УПК РФ. Отсюда следует, что такое немаловажное решение, как определение информации, подлежащей раскрытию в рамках проведения следствия, мы относим к компетенции руководителя следственного органа, так как ряд следователей, дознавателей, в силу ряда человеческих факторов, способны ошибочно совершать труд-

нопоправимые, а в редких случаях и неподлежащие исправлению действия, которые способны нанести «удар» как по следствию в рамках расследования конкретного уголовного дела, так и по следственным органам в целом.

Согласно ст. 310 Уголовного кодекса РФ, за разглашение данных предварительного расследования в нарушение подписки о неразглашении возможно привлечение к уголовной ответственности.

В то же время существуют два понятия («разглашение данных предварительного расследования» и «предание гласности данных предварительного расследования»), которые законом не запрещается использовать, если это делается установленным в ч. 4 ст. 161 УПК РФ способом, например, в рамках оглашения на открытом судебном заседании или самим следователем или дознавателем либо прокурором, даже путем размещения в средствах массовой информации или в сети Интернет, если это делается сугубо с целью информирования о совершенном преступном деянии и его расследовании либо предупреждении подобных совершенным деяниям. В частности, прокурор, может быть, обеспечителем прав потерпевшего на получение копий процессуальных документов [5. С. 340], в результате чего потерпевшему может стать известна некая информация, которая затрагивает интересы иных лиц, помимо его собственных интересов, однако при соблюдении процессуальной процедуры ответственности у прокурора в таком случае не возникнет.

Список литературы

1. Муратов К. Д. Хранение цифровой информации при формировании системы вещественных доказательств по уголовному делу // Санкт-Петербургский международный криминалистический форум: материалы международной научно-практической конференции. – Санкт-Петербург, 2024. – С. 349–353.
2. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.
3. Begishev I. R., Kirpichnikov D., Latypova E. Yu., Nechaeva E., Tasakov S. CRIMINAL LEGAL SUPPORT FOR SAFEGUARDING THE CITIZENS' DIGITAL RIGHTS // SHS WEB OF CONFERENCES: 3rd International Scientific Conference on New Industrialization and Digitalization (NID 2020). 2021. С. 02023.
4. Гончарова Н. Н., Латыпова Э. Ю., Гончаров Н. А. Проблемы проведения уголовно-процессуальных действий с участием иностранных граждан на российской территории, также в зданиях посольств и консульств России // Пробелы в российском законодательстве. 2021. Т. 14. С. 366–372.
5. Латыпова Э. Ю., Гильманов Э. М. Кирпичников Д. В. Роль прокурора в обеспечении права потерпевшего на получение копий процессуальных документов // Актуальные проблемы уголовного права, криминологии, уголовного процесса и уголовно-исполнительного права: теория и практика: материалы IX Международной научно-практической конференции // редколлегия: Э. Ю. Кузьменко [и др.]. – Тамбов: Издат. дом «Державинский», 2020. С. 339–347.
6. Asli M. R. Digital Trends of Criminology and Criminal Justice of the 21st Century // Journal of Digital Technologies and Law. – 2023. – № 1(1). – С. 235–250. <https://doi.org/10.21202/jdtl.2023.9>. EDN: ZMIRLT.

Е. М. Глянц,
преподаватель,

Казанский инновационный университет имени В. Г. Тимирязова

ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНИХ В ПРЕСТУПНУЮ ДЕЯТЕЛЬНОСТЬ ПОСРЕДСТВОМ ВЗАИМОДЕЙСТВИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Аннотация. В статье изучается вовлеченность несовершеннолетних в преступную деятельность путем коммуникации в сети Интернет как один из способов виктимизации несовершеннолетних. По результатам исследования сделан вывод о необходимости более глубокого изучения указанного способа виктимизации несовершеннолетних и обращено внимание на потребность в выработке специальных методов виктимологической профилактики.

Ключевые слова: цифровые технологии, киберпространство, несовершеннолетние, жертвы, потерпевшие, виктимизация, виктимологическая профилактика

INVOLVEMENT OF MINORS IN CRIMINAL ACTIVITIES THROUGH INTERACTION IN THE INTERNET SPACE

Abstract. The article examines the involvement of minors in criminal activities through communication on the Internet as one of the ways of victimization of minors. Based on the results of the study, it was concluded that there is a need for a deeper study of this method of victimization of minors and attention was drawn to the need to develop special methods of victimological prevention.

Keywords: digital technologies, cyberspace, minors, victims, victims, victimization, victimological prevention

Борьба с преступностью несовершеннолетних и противодействие вовлечению их в преступную деятельность – ключевые направления государственной политики правового государства. В Российской Федерации этим вопросам уделяется пристальное внимание.

Еще несколько лет назад несовершеннолетние вовлекались в совершение краж металла с дачных участков, грабежи и разбои, то сейчас несовершеннолетние вовлекают в незаконный оборот наркотиков, диверсии и другие тяжкие и особо тяжкие преступления. Опасность и масштаб преступлений, совершаемых несовершеннолетними, растет. В новостных лентах то и дело мелькают сообщения о поджогах подростками релейных шкафов на железной дороге, государственных учреждений и других преступлениях. Несовершеннолетние часто не самостоятельно принимают решение о совершении того или иного преступления. В преступную деятельность их вовлекают взрослые. И в этих случаях несовершеннолетние приобретают статус жертвы преступления. Происходит виктимизация несовершеннолетних.

Ответственность за вовлечение несовершеннолетних в преступную деятельность предусмотрена ст. 150 Уголовного кодекса Российской Федерации. Этой проблематике уделяется достаточно большое внимание в правовой док-

трине. В современном мире нет необходимости лично встречаться с несовершеннолетними, чтобы побудить их к совершению преступлений. Дистанционные методы гораздо эффективнее. Дети проводят много времени в интернет-пространстве, становясь жертвами преступлений, в том числе и вовлекаясь в преступную деятельность.

Общественная опасность вовлечения несовершеннолетних в преступную деятельность состоит в посягательстве на формирование личности несовершеннолетнего и в наставничестве на преступную деятельность [3].

26 мая 2023 года Конституционный Суд РФ опубликовал Постановление №26-П, принятое в соответствии со статьей 47.1 ФКЗ «О Конституционном Суде Российской Федерации». В Постановлении № 26-П разъясняется, что по смыслу статьи 150 УК РФ несовершеннолетний, вовлекаемый в совершение преступления любым способом, становится жертвой преступного посягательства со стороны взрослого. Он оказывается под пагубным влиянием, способным сформировать представление о допустимости преступного поведения, а также негативного отношения к правам других лиц, к ценностям общества и государства [6].

Действия взрослого лица могут быть облечены в различные формы. Российскими учеными выделено несколько способов вовлечения несовершеннолетних в преступную деятельность, например:

1. Обещание – обязательство совершить какие-либо действия в интересах несовершеннолетнего при условии выполнения им просьбы преступника.

2. Обман – введение несовершеннолетнего в заблуждение путем доведения до него информации, не соответствующей действительности, а также сокрытие каких-либо фактов.

3. Угроза – шантаж несовершеннолетнего путем распространения о нем сведений, порочащих его или его родных, запугивание причинением вреда жизни и здоровью [2. С. 123–127].

В сети Интернет эти способы встраиваются в общий механизм вовлечения несовершеннолетних в преступную деятельность посредством коммуникации в интернет-пространстве. Роль сети Интернет в формировании личности несовершеннолетних без преувеличения стоит признать ведущей. Интернет-контент создает, лепит личность подростка, как скульптор. Очень часто контент формирует у детей далеко не лучше качества. Это жестокость, пренебрежение к чувствам других людей, отрицание нравственных ценностей, правовой нигилизм, зависть и т. д. Особенности подросткового восприятия информации доказывают огромное влияние интернет-контента на формирование личностных качеств современного подростка, в том числе и разрушающее [2. С. 123–127].

Нами было проанализировано несколько уголовных дел по обвинению несовершеннолетних в совершении диверсий – поджогов релейных шкафов на железной дороге. В большинстве изученных уголовных дел несовершеннолетние были вовлечены в совершение этих преступлений взрослыми посредством коммуникации в сети Интернет. Во всех случаях лица, вовлекшие детей в преступную деятельность, установлены не были.

Анализ уголовных дел и изучение работ отечественных ученых позволяют выявить ряд закономерностей процесса вовлечения несовершеннолетних в совершение преступлений рассматриваемым способом. Для привлечения несо-

вершеннолетних к совершению преступлений в интернете активно применяются такие инструменты, как социальные сети и онлайн-игры. Контакт с подростками устанавливается через эти платформы, а дальнейшее взаимодействие происходит в ходе игр, общения в социальных сетях, тематических сообществах и даже группах по трудоустройству. Происходит так называемый рекрутинг подростков. Личности лиц, осуществляющих рекрутинг, тщательно законспирированы. Координация дальнейшей преступной деятельности несовершеннолетних также осуществляется в интернет-пространстве. Вовлечение в преступную деятельность несовершеннолетних в интернет-пространстве происходит анонимно, массово, быстро [1. С. 285–290] из-за того, что дети легко вовлекаются в преступную деятельность в Интернете, а злоумышленники умеют скрывать свою личность, вводя тем самым в заблуждение несовершеннолетнего.

Несовершеннолетние склонны к фантазиям, любопытству и игровому поведению из-за возрастных и психофизиологических особенностей. Например, некоторые подростки могут воспринимать преступную деятельность как своего рода квест. В ряде случаев недостаток жизненного опыта и уровень интеллектуального развития мешают им осознать опасность своих поступков и последствия, к которым они могут привести [1. С. 285–290]. Кроме того, несовершеннолетний лишен критики к подобному формату общения и чувствует себя в цифровом пространстве излишне уверенно.

Можно выделить следующие факторы, способствующие вовлечению несовершеннолетних в преступную деятельность путем взаимодействия в сети Интернет:

- непризнание авторитета взрослого, убежденность несовершеннолетнего своей большей осведомленности в данной сфере;
- правовой нигилизм;
- уверенность в собственной безнаказанности;
- отсутствие знаний об ответственности за свои действия;
- анонимность в интернет-пространстве;
- безнадзорность несовершеннолетних;
- влияние агрессивного интернет-контента на формирующуюся личность несовершеннолетнего.

С учетом исследованного материала можно сделать вывод о том, что необходимо выработать специальный механизм профилактики виктимизации несовершеннолетних в этой сфере.

Отечественными учеными предлагаются следующие пути решения рассматриваемой проблемы:

1. Совершенствование законодательной базы, регламентирующей вопросы профилактики безнадзорности и правонарушений несовершеннолетних [2. С. 123–127].

2. Мониторинг криминологической ситуации.

3. Выявление профиля жертвы данного вида преступной деятельности, с целью разработки эффективных мер виктимологической профилактики [4. С. 67–74].

4. Совершенствование информационного взаимодействия между правоохранительными органами и интернет-провайдерами [5. С. 191–195].

5. Повышение информированности несовершеннолетних об ответственности за противоправные деяния в интернет-пространстве. При этом следует учесть, что несовершеннолетние не прислушиваются к советам взрослых относительно того, что общение в интернет-пространстве может быть небезопасным. Это связано с тем, что дети считают себя более грамотными в вопросах интернет-взаимодействий, чем родители и педагоги. Поэтому несовершеннолетним необходим так называемый цифровой воспитатель, который бы пользовался авторитетом в их глазах.

Список литературы

1. Кузина Л. С. «Сетевой наркомаркетинг» как один из факторов вовлечения несовершеннолетних в незаконный оборот наркотиков // Вестник Воронежского института МВД России. 2020. № 4. С. 285–290.
2. Купирова Ч. Ш. Вовлеченность несовершеннолетних в преступные деяния: уголовно-правовой и криминологический аспекты проблемы // Вестник Российского университета кооперации. 2020. № 4(42). С. 123–127.
3. Майоров А. В. Криминализация вовлечения несовершеннолетних в преступную деятельность // Социальное управление. 2023. Т. 5, № 12.
4. Майоров А. В. Преступность несовершеннолетних: криминологический аспект ее состояния в российском обществе // Вестник Уральского института экономики, управления и права. 2020. №4. С. 67–74.
5. Мамаева А. Е. Меры предупреждения вовлечения несовершеннолетних в преступления посредством социальных сетей в зарубежных странах и в России // Закон и право. 2022. № 5. С. 191–195.
6. Постановление Конституционного Суда РФ от 25 мая 2023 г. № 26-П «По делу о проверке конституционности части четвертой статьи 150 Уголовного кодекса Российской Федерации и ряда положений статей 42, 45, 145, 146 и 222 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой граждан М. В. Золотаревой и В. В. Фроловой» // https://www.consultant.ru/document/cons_doc_LAW_447988 (дата обращения: 10.09.2024).
7. Постановление Пленума Верховного Суда РФ от 01.02.2011 № 1 (ред. от 28.10.2021) «О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних» // https://www.consultant.ru/document/cons_doc_LAW_110315 (дата обращения: 10.09.2024).

Ю. М. Графова,
аспирант,

Казанский инновационный университет имени В. Г. Тимирязова

СИСТЕМА ПРОФИЛАКТИКИ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация. Одной из самых актуальных проблем преступности во все времена является ее рост, напрямую зависящий от периода развития общества и дефицитов, которое оно переживает. Сейчас современное общество переживает мощный период цифровизации, который, как следствие, ведет к снижению логического анализа, происходящего на различных уровнях психики человека. В работе предложена система профилактических действий, направленных на предотвращение мошенничества с использованием социальной инженерии.

Ключевые слова: социальная инженерия, мошенничество, преступление, профилактика, уголовная ответственность

PREVENTION SYSTEM FRAUD USING SOCIAL ENGINEERING

Abstract. One of the most pressing problems of crime at all times is its growth, which directly depends on the period of development of society and the deficits that it is experiencing. Now modern society is going through a powerful period of digitalization as a stage of development, which in its negative manifestations is characterized by two deficits: a lack of socialization and a decrease in horizons, which, as a result, lead to a decrease in the level of logical analysis of what is happening at various levels of the human psyche. The paper proposes an author's system of preventive actions aimed at preventing fraud using social engineering.

Keywords: social engineering, fraud, crime, prevention, criminal liability

Цифровизация как этап развития общества явилась тем фактором, который позволил сформироваться новому виду преступности – киберпреступности. Известно, что на сегодняшний день преступники, специализирующиеся на цифровых видах преступлений, являются самыми неисследованными с точки зрения психологического и криминологического подходов. В настоящее время недостаточно исследований, позволяющих определить портрет киберпреступника, его психологические особенности, истинный мотив и цель, которые побуждают его к противоправным действиям.

Ввиду отсутствия портрета такого преступника отсутствует возможность для составления полного портрета жертвы подобных преступлений.

Портреты преступника и жертвы являются важной составляющей частью при формировании правил профилактики таких преступлений, однако отсутствуют соответствующие исследования, которые позволяли бы установить четкие цели и причины, побуждающие преступника к совершению преступления.

На сегодняшний день одним из основных видов противоправных деяний в рассматриваемой сфере является мошенничество с использованием социальной инженерии, которая требует более детального изучения в психолого-криминологическом и уголовно-правовом разрезах.

В связи с этим представляется логичным разделить систему профилактических действий, направленных на предотвращение мошенничества с использованием социальной инженерии, на четыре основные группы мер:

1. Образовательно-просветительские меры, направленные на обучение граждан, лиц без гражданства и сотрудников организаций, учреждений, предприятий независимо от форм собственности новым методам противодействия социоинженерным атакам в целях повышения культуры информационной безопасности и поддержания должного уровня цифровой гигиены.

2. Технологические (предупредительно-охранительные) меры, направленные на тщательную проверку входящих ссылок и иной цифровой информации, поступающей на любого рода средства связи, а также не использование повышенной степени защиты своей личной цифровой информации.

3. Правовые меры, направленные на разработку норм, устанавливающих ответственность за такого рода преступления, защиту прав потерпевших лиц, совершенствование имеющегося законодательства, регулирующего правоотношения в указанной сфере, контролирующие исполнение такого законодательства и на разных уровнях его применения.

4. Психологические меры, направленные на профилактику стресса.

Указанные группы мер крайне важны для эффективной выработки профилактических мер противодействия мошенничеству с использованием социальной инженерии.

В подавляющем большинстве преступлений, связанных с передачей личных данных преступникам уровень критического мышления у жертв снижен до минимального значения. Критическое мышление – это умение всесторонне анализировать информацию и делать обоснованные, объективные выводы [1]. Также под критическим мышлением понимают способность ставить под сомнение любую информацию, в том числе собственные убеждения.

Ключевыми признаками критического мышления являются способность наблюдать; концентрироваться и сохранять внимание и др.

Несмотря на наличие врожденных личностных характеристик, при общих вводных каждый способен увеличить уровень своего критического мышления. Существуют разнообразные способы, в зависимости от темперамента и склонностей человека к усвоению информации, повысить свой уровень критического мышления. Прибегая к давно известным формам обработки информации, можно выделить межличностный подход, включающий в себя дискуссии, обсуждения, и индивидуальный, куда входят самостоятельный поиск и анализ информации, работа с найденной информацией, построение логических рассуждений и выводов, аргументация при дискуссии, обнаружение ошибок в мышлении, в том числе собственных.

Развитие и формирование критического мышления до высокого уровня позволяют оценивать криминогенную обстановку и принимать управленческие решения в целях минимизации последствий и предотвращения социоинженерных атак.

Важным нюансом является тот факт, что главным инструментом преступлений в социальной инженерии является манипуляция на эмоциях и конструирование ситуаций, которые могут выглядеть совершенно реальными.

Формирование достаточного уровня критического мышления увеличит способность жертвы в процессе осознания рисков при контакте с кибермошенниками прежде, чем предоставлять конфиденциальную информацию или совершать финансовые операции.

Завершая рассуждения, подчеркнем, что для эффективной профилактики мошенничества с использованием социальной инженерии предлагаем использовать все четыре меры системно, комплексно и неразрывно. Одновременное использование этих мер позволит снизить вероятность совершения социоинженерной атаки злоумышленниками.

Список литературы

1. Садова А.Р., Хиль Ю.С., Пащенко Т.В., Тарасова К.В. Измерение критического мышления взрослых: методология и опыт разработки // Современная зарубежная психология. 2022. Т. 11, № 4. С. 115–116.

В. В. Денисович,

кандидат юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирязова,
Южно-Уральский государственный университет
(национальный исследовательский университет)

КРИМИНОЛОГИЧЕСКИЕ И ЭТИЧЕСКИЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ МЕТАВСЕЛЕННЫХ

Аннотация. Суть использования этических категорий в цифровых правоотношениях сводится к тому, чтобы определить рамки публичных дискуссий относительно содержания на основе идей признания и социальной справедливости. Востребованность концепции этических основ в использовании виртуальных пространств базируется на том, что этика позволяет сформировать направление будущего нормотворчества в области использования метавселенных. Новые нормы морали могут стать основой для формирования современных нормативных актов.

Ключевые слова: метавселенные, криминологические риски метавселенных, виртуальное пространство, цифровой аватар человека, метagalлактики

ETHICAL BASES OF META-UNIVERSES USE

Abstract. The essence of the use of ethical categories in digital legal relations comes down to defining the framework of public discussions, regarding the content on the basis of the ideas of recognition and social justice. The demand for the concept of ethical foundations in the use of virtual spaces is based on the fact that ethics allows to form the direction of future normativity in the use of meta-universes. New norms of morality can become the basis for the formation of modern normative acts.

Keywords: metavillages, criminological risks of metavillages, virtual space, digital human avatar, metagalactics

Введение. Использование в юриспруденции смежных категорий и понятий провоцирует споры о возможности регулирования данных общественных отношений нормами публичного и частного права. Понятием «этика» обычно называют совокупность идей, которые объясняют отношение общественности к таким оценочным категориям, как справедливость, социальная справедливость, стигматизация, признание права, непризнание права.

У данного термина давняя история, его часто используют для расширения границ правового регулирования различных институтов в области юриспруденции. В современной Российской Федерации возникла потребность этико-нормативного регулирования для разработки и использования новых технологий, возникающих в сфере уголовно-правовых отношений.

Основная часть. Указанный выше подход свидетельствует о том, что, если неправильно выстроить систему этических ценностей в государстве, система ценностей становится нестабильной, институты права подвергаются критике. Отношения между различными материальными и идеальными составляющими культурного поля действия носят системный характер; преобразования в одной части системы отражаются в любой другой части. Чтобы стать компонентом культурного поля действия, необходимо пройти через определенные ментальные операции. Некоторые компоненты материального потока остаются за пределами восприятия человека, как бы вне его интенционального мира. Социокультурная среда – это интенциональный мир.

Человек все чаще стал использовать VR-технологии, метавселенные для достижения своих поставленных целей. Для метавселенных ключевым этическим правилом является осознанность при использовании их ресурсов человеком, иначе возникает риск совершения преступления. Важно разработать программы по формированию осознанного использования технологий метавселенных, в которые будут включены правила использования этих цифровых технологий [2].

В метавселенных широко используются блокчейн+технологии. Повсеместное развитие технологии блокчейн вышло далеко за пределы финансового сектора. Эта тенденция охватила еще одну стремительно развивающуюся сферу – игровую. Массовая интеграция и внедрение технологии блокчейн в игровую индустрию метавселенных неуклонно меняют облик этой сферы и правила, которые не пересматривались годами. Часто приходится слышать о блокчейне и о том, что он делает для финансов, однако многим до сих пор не ясно, какие преимущества может дать блокчейн и как именно он может изменить принципы игры. В данном контексте развитие норм этики поведения может усилить качество правовой разработки системы блокчей технологий метавселенных.

Блокчейн предоставляет геймерам прямой контроль над их внутриигровыми предметами и различными активами, которые были накоплены в процессе игры. Все внутриигровые предметы и активы могут быть токенизированы с последующим переходом на NFT, если украшать их уникальными атрибутами. Блокчейн позволяет геймерам владеть внутриигровыми предметами и не бояться, что разработчики оштрафуют их и отберут все предметы [3]. В то же время NFT можно переносить из одной игры в другую, при этом игрок будет единственным владельцем персонажа и снаряжения, заработанного в процессе игры.

Основной криминологической и этической проблемой реализации метавселенных является риск возникновения болезненной зависимости от нахождения в условиях VR-пространства, когда человек игнорирует происходящее в реальности, предпочитая метавселенную. Очевидными представляются следующие выводы. Пока человек работает с первыми версиями метавселенных, они будут подконтрольны. Сложности возникнут тогда, когда будут использоваться самопрограммируемые метавселенные, которые не поддаются воле человека. Необходимо также определиться с тем, зависит ли метавселенная от своего создателя.

Заключение. По мере расширения использования цифровизации общества будет существенно меняться деятельность человека как в реальной, так и в виртуальной среде. В основе этих изменений лежат преобразования, происходящие в цифровом сознании, цифровых отношениях и цифровой деятельности личности [3].

Если рассматривать метавселенную как прототип реальности, то значит должны действовать нормы о правонарушениях и в виртуальной среде. Разбирая вопрос правовых аспектах подробнее, следует разобрать вопрос о деликтном праве [1]. Пока метавселенные рассматриваются исключительно в связке с реальным миром без учета их особенностей [2].

Цифровые технологии предоставляют новые возможности для осуществления прав человека, но они слишком часто используются и для нарушения этих прав. Законодательству еще предстоит долгий путь совершенствования для полноценного регулирования правоотношений в метавселенных [3].

Список литературы

1. Baranzke H. Shortcuts in the Animal Rights Discussion On the Question of the Legal Personality of Animals from an ethical Point of View // *Zeitschrift für Evangelische Ethik*. 2019. Vol. 63, Issue 1. P. 21-33. DOI: 10.14315/zee-2019-630105.
2. Clark M. D. Drag Them: A brief etymology of so-called “cancel cul-ture” // *Communication and the Public*. 2020. Vol 5, Issue 3–4. P. 88-92. DOI:10.1177/2057047320961562.
3. Бегишев И. Р., Денисович В. В., Сабитов Р. А., Пасс А. А., Скоробогатов А. В. Уголовно-правовое значение метавселенных: коллизии в праве // *Правопорядок: история, теория, практика*. 2023. № 4(39). С. 58–62.
4. Бегишев И. Р., Жарова А. К., Громова Е. А., Залойло М. В., Филипова И. А., Шутова А. А. «Цифровой поворот» в юридических исследованиях // *Journal of Digital Technologies and Law*. 2024. Т. 2, № 2(1). С. 22–25.
5. Зайцева А. М. Правовые аспекты метавселенной // *Традиции и новации в системе современного российского права: материалы XXII Международной научно-практической конференции молодых ученых. Том 3: Секция «Метавселенная: философские, духовные и правовые проблемы и их решения»*. Москва: Издательский центр Университета имени О. Е. Кутафина (МГЮА), 2023. 450 с.
6. Нойманн Э. Глубинная психология и новая этика. Человек Мистический. М.: Азбука, 2008. 256 с.
7. Сахаров А. Д. Размышления о прогрессе, мирном сосуществовании и интеллектуальной свободе. URL: <https://www.sakharov-archive.ru/sakharov/works/razmyshleniya> (дата обращения: 01.05.2021).

В. В. Денисович,
кандидат юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирязева,
Южно-Уральский государственный университет
(национальный исследовательский университет)

КРИМИНОЛОГИЧЕСКОЕ ИЗМЕРЕНИЕ МЕТАВСЕЛЕННЫХ

Аннотация. Использование цифровых технологий и внедрение WEB 3.0, признание необходимости использования трехмерного Интернета для насущных потребностей человека обусловили необходимость изменить существующие институты и системы права. Виртуальная реальность перестает быть только футурологической темой для обсуждения. Современные профессиональные сообщества нуждаются в новом видении механизмов правового регулирования общественных отношений в трехмерном пространстве, поскольку оно не только давно существует, но в нем уже есть правоотношения, которые влекут сложные группы правовых отношений, которые могут как помочь человеку в решении его целей и задач, так и навредить. В статье представлен анализ основных криминологических рисков, которые могут повлиять на формирование криминологических показателей преступности в Российской Федерации в будущем, а также повысить уровень социальной напряженности в обществе.

Ключевые слова: метавселенные, криминологические риски метавселенных, виртуальное пространство, цифровой аватар человека, метагаллактики, криминологические риски, цифровые технологии

THE CRIMINOLOGICAL DIMENSION OF META-UNIVERSES

Abstract. The use of digital technologies and the introduction of WEB 3.0, the recognition of the need to use the three-dimensional Internet for pressing human needs has made it necessary to change the existing institutions and systems of law. Virtual reality ceases to be only a futurological topic for discussion. Modern professional communities need a new vision of the mechanisms of legal regulation of social relations in three-dimensional space, since it has not only existed for a long time, but there are already legal relations in it, which entail complex groups of legal relations that can both help and harm a person in solving his goals and objectives. The article presents an analysis of the main criminological risks that may affect the formation of criminological indicators of crime in the Russian Federation in the future, as well as increase the level of social tension in society.

Keywords: metavillages, criminological risks of metavillages, virtual space, human digital avatar, metagalactics, criminal risks, digital technologies

Введение. Неоднократно в теории обсуждалось, что метавселенная пока не имеет четких правовых границ. Обозначим ряд вопросов, которые требуют детального рассмотрения и обсуждения, прежде чем будут приняты кодифицированные акты, в том числе Цифровой кодекс Российской Федерации 2025 года. Во-первых, возникает вопрос о том, какие правовые механизмы должны применяться в метавселенной и как следует выстроить систему права, обосновать

взаимодействие между отраслями права, так как ряд вопросов просто на просто исчезнет из сферы правового регулирования, так как в виртуальном пространстве речь идет о цифровом аватаре человека, а не о нем самом. Во-вторых, ведутся дебаты о том, способны ли нынешние регулирующие органы в физическом мире эффективно регулировать метавселенную с помощью существующих законов и нормативных актов, но при этом нет четкого ответа на вопрос: кто, как, какой государственный орган, в каком правовом статусе будет контролировать сами метавселенные, правовые отношения внутри метавселенной, правовые отношения, складывающиеся в результате использования пространства метавселенной, а также в отношении самой метавселенной. В-третьих, возникает вопрос о том, как бороться с преступлениями, совершаемыми в виртуальной среде, и следует ли рассматривать их в рамках существующего деликтного или уголовного права, или же следует создать отдельную группу преступлений. Российская Федерация сейчас находится на этапе формирования терминологической базы метавселенных и правил поведения в виртуальной среде. Для решения этих вопросов необходимо проанализировать криминологические риски существования и использования всех возможностей метавселенных в жизни человека.

Основная часть. С 2019 по первое полугодие 2024 года было издано более 1000 научных трудов в России по теме социальной обусловленности метавселенных и правил общения в них.

Метавселенные – это совершенно новое явление не только в IT-сфере, но и в социальной среде, можно выделить ряд первоочередных проблем правового характера, которые нуждаются в урегулировании уже сейчас: проблемы, связанные с противоправным поведением, таким как мошенничество, хищение данных, нарушение конфиденциальности, кибербуллинг, насилие над аватаром и др. Кроме проблем правового регулирования и ответственности за подобные деяния, возникает вопрос о способах сбора цифровых доказательств, ведения расследования и т.д.

В подтверждение обоснованности и особой важности исследований метавселенных в современной реальности цифрового права России обратимся к статистическим данным. Сколько времени вы проводите каждый день прикованными к светящемуся экрану своего компьютера или смартфона? Если верить последним глобальным исследованиям, человек в среднем каждый день проводит за экраном смартфона или персонального компьютера около 6 часов.

Согласно данным, дети в возрасте 8–12 лет проводят за экранами 4–6 часов в день, в то время как подростки проводят за экранами до 9 часов – статистика, которая, как также показывают последние данные и исследования, может оказывать неблагоприятное воздействие на их психическое и физическое здоровье. В третьем квартале 2024 года глобальная сеть Интернет использовалась 5,44 млрд человек (это более 2/3 всего населения земного шара). В период с 2023 по 2024 год среднее время, проведенное пользователями Интернета в 18 странах, увеличилось, при этом Израиль лидирует:

1. Израиль (+26 минут).
2. Великобритания (+21 минута).
3. Япония (+19 минут).
4. Австралия (+16 минут).

5. США (+14 минут).
6. Россия (+13 минут).
7. Малайзия (+12 минут).
8. Индия (+12 минут).
9. Гонконг (+11 минут).
10. Новая Зеландия (+11 минут).
11. ОАЭ (+9 минут).
12. Чехия (+9 минут).
13. Германия (+8 минут).
14. Тайвань (+6 минут).
15. Швейцария (+6 минут).
16. Бельгия (+6 минут).
17. Нидерланды (+6 минут).
18. Норвегия (+2 минуты).

Все время пользователей по всему миру в возрасте от 16 до 64 лет в 2024 году – на разных платформах и устройствах – составляет 6 часов 35 минут ежедневно, хотя, как мы увидим ниже, не все страны используют экранное время одинаково или для одних и тех же целей [12].

Также вместе с увеличением числа пользователей в метавселенных приобретает важность вопрос профилактики указанных нарушений. Важной составляющей регулирования метавселенных является сознательность пользователей относительно их поведения и действий в виртуальных мирах. Необходимо развивать программы и образовательные инициативы, направленные на повышение уровня социальной сознательности и этики в метавселенных [10, 11].

В научной среде также увеличилось число ученых, профессионально исследующих сферу метавселенных и виртуального пространства в целом. С 2021 года по предложенной тематике опубликовано 59 научных публикаций: в 2021 году – 11, в 2022 – 17, в 2023 – 28, за первый квартал 2024 года – 3. Среди ключевых слов по данной тематике наиболее часто встречаемыми являются: метавселенные, виртуальное пространство, киберпространство, кибербезопасность. Необходимо отметить, что в публикациях 2019–2021 годов чаще всего авторы рассматривали проблемы кибербезопасности и киберпространства, возможности совершения преступлений с использованием информационных технологий.

Основная масса публикаций по метавселенным и виртуальным правам человека в метасреде появилась в период 2022–2023 год, когда активно начали развиваться теории цифрового права, цифровые технологии, на практике с положительной стороны себя зарекомендовали виртуальные способы реализации правомочий человека.

С философской точки зрения при разработке, использовании и внедрении метавселенных существуют следующие риски:

- 1) не сформулированы критерии и ограничения влияния воздействия на участников метавселенной;
- 2) не определены критерии разграничения виртуальной реальности и повседневной;
- 3) не определены и процессуально не разработаны способы защиты человека от ситуаций, когда он спутает виртуальное пространство и реальное;

4) не определены новые модели взаимодействия людей в метавселенной, а также не определены критерии дублирующих форм поведения.

Основной этической и криминологической проблемой реализации метавселенных является риск возникновения патологической зависимости от виртуального мира, когда человек игнорирует происходящее в реальности, предпочитая метавселенную (данный тезис подтвержден в 63% научных публикаций по этике искусственного интеллекта). Очевидными представляются следующие выводы. Пока человек работает с первыми версиями метавселенных, они будут подконтрольны. Сложности возникнут тогда, когда будут использоваться самопрограммируемые метавселенные, которые не поддаются воле человека. Необходимо также определиться с тем, зависит ли метавселенная от своего создателя.

В условиях виртуальной среды также существуют правила общения, однако нет классического понимания жизни и смерти. Возникает необходимость разработать комплекс норм права, определяющих, как привлекать к ответственности человека, чей аватар совершил преступление в виртуальной среде, но как физический – субъект не виновен, а также методику правового поведения, если человек физически умер, а аватар «жив». Необходимо определиться, как применять санкцию к аватару, если сроки привлечения к ответственности в реальной виртуальной жизни не совпадают. Необходимо предусмотреть нормы, согласно которым человек может отследить, какие санкции применяются к его аватару на основе социального инжиниринга, но при этом понимать, как это сказывается на его физическом состоянии.

По мере расширения использования цифровизации общества будет существенно меняться деятельность человека как в реальной, так и в виртуальной среде. В основе этих изменений лежат преобразования, происходящие в цифровом сознании, цифровых отношениях и цифровой деятельности личности [4. С. 5].

Если рассматривать метавселенную как прототип реальности, то значит должны действовать нормы о правонарушениях и в виртуальной среде. Разбирая вопрос правовых аспектах подробнее, следует разобрать вопрос о деликтном праве. В настоящее время действует Закон КоАП РФ, статья 5.61 «Оскорбление», в связи с которым уже сейчас можно привлечь лицо к ответственности за оскорбление в сети Интернет [12]. Пока метавселенные рассматриваются исключительно в связке с реальным миром, если законами или правилами среды не установлены какие-либо исключения [1. С. 8].

Присоединяемся к точке зрения авторов, считающих, что мы можем отметить, что права человека должны соблюдаться в интерактивном режиме точно так же, как и в физическом мире. Цифровые технологии предоставляют новые возможности для осуществления прав человека, но они слишком часто используются и для нарушения этих прав. Законодательству еще предстоит долгий путь совершенствования для полноценного регулирования правоотношений в метавселенных [2. С. 23].

Заключение. Внедрение метавселенных в реальную жизнь человека представляется прогрессивной идеей, не лишенной недостатков. Много будет зависеть от эффективной реализации каждого этапа внедрения и использования виртуальных пространств. Например, могут быть платные сервисы, доступные

не всем гражданам, кроме того, сама метавселенная – дорогостоящая цифровая технология. Первоначально будут ограничены возможности использования VR-оборудования [3. С. 142].

Таким образом, прежде чем внедрять активно метавселенные, нужно найти новый баланс между реальным и виртуальным. Виртуальный мир включает в себя гораздо больше, чем реальный, именно этот фактор прямо указывает на необходимость создания новой базы в области законодательного регулирования метавселенных.

Список литературы

1. Бегишев И. Р., Денисович В. В., Сабитов Р. А., Пасс А. А., Скоробогатов А. В. Уголовно-правовое значение метавселенных: коллизии в праве // Правопорядок: история, теория, практика. 2023. № 4 (39). С. 58–62.
2. Бегишев И. Р., Жарова А. К., Громова Е. А., Залоило М. В., Филипова И. А., Шутова А. А. «Цифровой поворот» в юридических исследованиях // Journal of Digital Technologies and Law. 2024. Т. 2, № 2 (1). С. 22–25.
3. Зайцева А. М. Правовые аспекты метавселенной // Традиции и новации в системе современного российского права: материалы XXII Международной научно-практической конференции молодых ученых. Том 3: Секция «Метавселенная: философские, духовные и правовые проблемы и их решения». Москва: Издательский центр Университета имени О. Е. Кутафина (МГЮА), 2023. 450 с.
4. Лихачев Н. А. Нематериальное пространство как новая форма места совершения преступления: доктринальный аспект // Юридические исследования. 2024. № 4. С. 1–8.
5. Speech of the President of the Russian Federation V.V. Putin at the conference "Journey into the world of artificial intelligence" [Web resource]. URL: <https://www.ntv.ru/video/2057923> (дата обращения: 05.08.2024).
6. Experiments in Metaverse and Their Applications to Collaborative Projects: The Framework and Its Significance. 24th International Conference on Knowledge-Based and intelligent Information & Engineering Systems. Tokyo, Japan.
7. Forecast on cyber threats in the consumer segment for 2023 [Web resource]. – URL: <https://securelist.ru/consumer-threats-2023/106215/> (дата обращения: 05.08.2024).
8. Kim E., Park, Y., & Jo, S. Educational Applications of Metaverse: Possibilities and Limitations // JEEHP (Journal For Educational Evaluation for Health Professions). 2021. № 18 (32).
9. Maslenko D. What is a metaverse and why is everyone talking about it [Web resource]. URL: <https://trends.rbc.ru/trends/industry/61449fa89a7947159f1df418>
10. Open Challenges. URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9667507>, VOLUME 10 (2022) (дата обращения: 05.08.2024).
11. Statistics of visits to the Fortnite [Web resource]. URL: <https://activeplayer.io/fortnite/>; Statistics of visits to the Roblox [Web resource]. URL: [metaverse: https://activeplayer.io/roblox](https://activeplayer.io/roblox) (дата обращения: 05.08.2024).

12. Speech of the President of the Russian Federation V. V. Putin at the conference "Journey into the world of artificial intelligence" [Web resource]. URL: <https://www.ntv.ru/video/2057923> (дата обращения: 05.08.2024).

Д. Е. Дроздов,

кандидат юридических наук,

Калужский государственный университет имени К. Э. Циолковского

ЦИФРОВЫЕ СРЕДСТВА ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПНОСТИ

Аннотация. Статья посвящена исследованию цифровой преступности, зафиксированной в официальной статистике как преступления, совершенные с помощью информационно-коммуникационных технологий или в области компьютерной информации. Отмечается рост количества зарегистрированных преступлений, что указывает на вероятный дальнейший рост в будущем. Также представлены данные об увеличении числа пользователей Интернета и времени, проводимого ими в сети. Определены некоторые субъекты предупреждения цифровой преступности. Предложены комплексные меры с повышением роли государственных органов.

Ключевые слова: преступность, Интернет, профилактика, статистика, меры предупреждения, субъекты профилактики, объекты профилактики

DIGITAL CRIME PREVENTION TOOLS

Abstract. The article is devoted to the study of digital crime, recorded in official statistics as crimes committed using information and communication technologies or in the field of computer information. There has been an increase in the number of reported crimes, which indicates a likely further increase in the future. Data on the increase in the number of Internet users and the time they spend online are also presented. Some subjects of digital crime prevention have been identified. Comprehensive measures have been proposed, with an increased role for government agencies.

Keywords: crime, Internet, prevention, statistics, prevention measures, subjects of prevention, objects of prevention

Введение. Согласно Единому годовому отчету VK за 2023 год, средняя дневная аудиторная нагрузка на сервисы компании составляла 76 миллионов пользователей (+13% к предыдущему году). В четвертом квартале 2023 года месячная аудитория составляла 87,7 миллиона пользователей России в месяц [1]. В соответствии с данными обзора российского IT-рынка за 2023 год среднемесячное число пользователей в России составляет 102,7 миллиона человек. 84% населения пользуется Интернетом, а 83% делает это ежедневно [2]. Фактически различными интернет-технологиями пользуется подавляющее большинство населения государства.

Основная часть. Статистические данные позволяют спрогнозировать увеличение числа пользователей и времени, проводимом в Сети, на ближайшие

годы. С большой долей вероятности они составят массив латентной преступности, поскольку не причиняют фактического вреда потерпевшим.

Некоторые тенденции роста исследуемой преступности нашли свое отражение в официальных статистических данных МВД России. В 2021 году темп прироста составил +1,4%, в 2022 – +0,8%, однако в 2023 произошел очередной рост на 29,7% до 676 951 преступления [5]. Изложенное свидетельствует о необходимости системного подхода к предупреждению преступлений, совершенных в цифровой среде, и определении ключевых объектов и субъектов профилактической деятельности. Вовлеченность подавляющего большинства населения страны в интернет-пространство предполагает его разделение по возрастному признаку. Эти две категории населения являются приоритетными объектами профилактического воздействия, что, однако, не исключает иные категории граждан из сферы профилактики.

Среди субъектов профилактического воздействия выделяются несколько групп. Во-первых, правоохранительные органы, непосредственно осуществляющие деятельность по противодействию преступности. Во-вторых, иные федеральные органы исполнительной власти, осуществляющие нормативно-правовое регулирование, а также профилактическое воздействие в границах полномочий. Одно из центральных занимает Министерство цифрового развития, связи и массовых коммуникаций РФ, которое может выступать координатором деятельности других органов государственной власти. В-третьих, различные общественные объединения, к примеру «Лига безопасного интернета», основной целью которой является создание безопасного интернет-пространства на территории страны. Согласно официальным данным сайта, объединение занимается проведением тематических уроков в образовательных учреждениях, оказывает методическую помощь педагогам, проводит акции и конкурсы, что, несомненно, обладает профилактическим эффектом, нацеленным на наиболее активную группу пользователей виртуального пространства. Кроме того, по состоянию на 06 сентября 2024 года, ее представители участвовали в разработке четырех федеральных законов, направленных на защиту прав и интересов пользователей российского сегмента интернета, а в настоящее время принимают участие в создании Проекта новой концепции информационной безопасности детей в Российской Федерации [10]. К сожалению, сведений о наименовании федеральных законов на сайте не содержится, а Концепция информационной безопасности детей в РФ утверждена в прошлом году Распоряжением Правительства РФ от 28 апреля 2023 года №1105-р [11]. В-четвертых, специализированные организации, занимающиеся разработкой программного обеспечения, для комплексной безопасности физических и юридических лиц. К примеру, среди российских выделяется «Лаборатория Касперского» – международная компания в сфере информационной безопасности. Согласно данным официального сайта организация активно занимается образовательной деятельностью школьников и студентов колледжей [12]. В-пятых, социальные сети, обеспечивающие безопасность ресурсов своих и пользователей.

Далеко не полный приведенный перечень субъектов свидетельствует о важности предупредительной деятельности и вовлеченности в процессы не только государственного аппарата, но и институтов гражданского общества.

Многообразие субъектов профилактической деятельности обуславливает необходимость классификации средств (мер) предупреждения цифровой преступности:

на нормативно-правовые, определяющие общие основы регулирования общественных отношений и реагирования на возникающие угрозы;

организационные, обеспечивающие функционирование отдельных субъектов и их взаимодействие;

технические, создающие безопасную среду и защищающие ее от угроз.

Заключение. Перспектива совершенствования системы противодействия цифровой преступности определяется комплексностью решения проблем безопасности с повышением роли государства. Необходимость государственного участия в разработке антивирусного и иного программного обеспечения, либо контроля за деятельностью соответствующих организаций определяется массовой вовлеченностью населения в виртуальную среду, движением значительных денежных средств. Актуальной остается разработка нейросетей и их обучение для выявления, предупреждения, пресечения подготавливаемых и совершаемых преступлений и административных правонарушений, не только цифрового характера.

Список литературы

1. Единый годовой отчет VK за 2023 год. URL: <https://vk.company/ru/investors/results> (дата обращения 04.09.2024).
2. Обзор российского IT – рынка за 2023 год. URL: <https://vk.company/ru/investors/results> (дата обращения 04.09.2024).
3. Состояние преступности в России за январь – декабрь 2019 года. URL: <https://мвд.рф/reports/6> (дата обращения 04.09.2024).
4. Состояние преступности в России за январь – декабрь 2020 года. URL: <https://мвд.рф/reports/5> (дата обращения 04.09.2024).
5. Состояние преступности в России за январь – декабрь 2021, 2022, 2023 годов. URL: <https://мвд.рф/reports> (дата обращения 04.09.2024).
6. Вопросы Министерства внутренних дел Российской Федерации: Указ Президента РФ от 01.03.2011 № 248 (ред. от 30.09.2022) // СПС «Консультант плюс» (дата обращения: 04.09.2024).
7. Официальный сайт Следственного комитета РФ. URL: <https://sledcom.ru/press/smi/item/1422678> (дата обращения: 04.09.2024).
8. О структуре федеральных органов исполнительной власти: Указ Президента РФ от 15 мая 2018 г. №2 15 (ред. от 21.01.2020) // СПС «Консультант плюс» (дата обращения: 04.09.2024).
9. О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации: Постановление Правительства РФ от 02.06.2008 № 418 (ред. от 15.03.2024) (с изм. и доп., вступ. в силу с 01.09.2024) // СПС «Консультант плюс» (дата обращения: 04.09.2024).
10. Лига безопасного интернета. URL: <https://ligainternet.ru/o-nas> (дата обращения: 06.09.2024).
11. Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Прави-

тельства РФ 02.12.2015 №2471-р: Распоряжение Правительства РФ от 28.04.2023 № 1105-р // СПС «Консультант плюс» (дата обращения: 06.09.2024).

12. Лаборатория Касперского. URL: <https://kaspersky.ru/about/company> (дата обращения: 06.09.2024).

Е. А. Дубынин,
кандидат юридических наук, доцент,
Сибирский федеральный университет
А. А. Берняцкий,
студент,
Сибирский федеральный университет

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНОМ ПРОЦЕССУАЛЬНОМ ПРАВЕ

Аннотация. Цель и задачи исследования заключаются в изучении вопроса применения нейросетевых моделей в уголовном процессуальном праве с учетом правоприменительной практики и теории уголовного процесса в России и за рубежом с точки зрения их положительного или отрицательного влияния на развитие этой отрасли права.

Ключевые слова: право, цифровые технологии, уголовный процесс, цифровизация уголовного процесса, искусственный интеллект, нейросети, принципы уголовного процесса, эмпатия, зарубежный опыт

THE USEGE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEDURAL LAW

Abstract. The purpose and objectives of the research are to study the application of neural network models in criminal procedural law, subject to law enforcement practice and theory of criminal procedure in Russia and abroad in terms of their positive or negative impact on the development of this branch of law. The conducted research touches upon the concepts of the use of artificial intelligence, the potential for its development, and the attitude of "alive" workers to modern technologies.

Keywords: law, digital technologies, criminal procedure, digitalization of criminal proceedings, artificial intelligence, neural networks, principles of criminal procedure, empathy, foreign experience

Введение. В эпоху развития цифровых технологий фактически отсутствуют направления деятельности в государстве, которых бы не коснулся процесс цифровизации. Не обошел этот процесс и сферу права. Уголовное процессуальное право, задачи и функции которого заключаются в обеспечении защиты прав и свобод граждан, эффективном расследовании преступлений и обеспечении справедливости в ходе уголовного судопроизводства, также не может оставаться в стороне от использования инновационных технологий. При этом вопросы использования таких технологий, в силу специфики уголовного судопроиз-

водства, являются наиболее чувствительными, требуют особой оценки, научного и законодательного регламентирования.

Основная часть. Так, некоторые технологии способны реализовывать определенные элементы мыслительной и когнитивной функции человека. «Связь ряда технологий с интеллектуальной деятельностью привела к объединению их единым понятием «искусственный интеллект»» (далее ИИ) [7. С. 320–327].

Не секрет, что ИИ способен анализировать большие объемы данных, обрабатывать информацию, производить достоверные прогнозы и предоставлять важную поддержку в принятии решений. Особенностью ИИ является то, что он способен к обучению на основании представленных ему материалов и поставленных задач, а в последующем и к самообучению и саморазвитию.

Вместе с тем говорить о способности ИИ понимать, познавать, изучать, воспринимать и перерабатывать (запоминать, передавать, использовать) внешнюю информацию на уровне возможностей человека преждевременно, такая технология еще не создана.

Для понимания возможностей использования технологий искусственного интеллекта (ИИ) в уголовном процессуальном праве, важно осознавать основные характеристики ИИ, выделенные В. В. Глимеидой [7. С. 320–327]:

1. ИИ представляет собой информацию, реализованную в виде программы или алгоритма.

2. Интеллектуальные системы базируются на логической обработке данных и информации, выступая в качестве метатехнологии, способной эффективно преобразовывать любую информацию и принимать на ее основе оптимальные решения.

3. ИИ является самообучающимся алгоритмом, который при обработке информации стремится делать это наиболее рациональным способом, с каждым разом достигая лучших результатов.

4. ИИ способен лишь имитировать мыслительную деятельность человека.

Исходя из указанных признаков, полагаем возможным сформулировать основные концепции применения ИИ в уголовном процессуальном праве.

1) искусственный интеллект является автономной единицей, способной самостоятельно выполнять ряд задач (так называемый «сильный ИИ»). Действительно, суть искусственного интеллекта в том, чтобы имитировать мозговую деятельность человека. А значит, теоретически возможен исход, при котором ИИ будет самостоятельно осуществлять расследования по уголовным делам, выносить решения по уголовным делам и т.п.;

2) искусственный интеллект является универсальным инструментом в руках квалифицированных специалистов, который способен значительно облегчить ряд процедурных процессов (так называемый «реальный» или «слабый ИИ»).

Например, ИИ может применяться в качестве вспомогательного средства в уголовном судопроизводстве как при исследовании, так и при реализации механизма доказывания, стать универсальной поисковой системой. А в сочетании с большими данными (BigData) ИИ способен поставить процесс поиска доказательств в ходе расследования на качественно новый уровень, выявлять скрытые взаимосвязи в событиях и поведении лиц.

Проведенный сравнительный анализ опыта зарубежных стран в области использования ИИ в сфере права, позволяет сделать вывод о том, что наиболее актуальным в настоящее время в мире является второй подход к использованию ИИ.

Так, наиболее широко такие технологии внедряются в области гражданского судопроизводства [13. С. 1367]. Особенно в этом продвинулся Китай, где с 2016 года внедрены собственные разработки ИИ. В настоящее время ряд судебных заседаний проходит непосредственно в системе Интернет с использованием программы WeChat, где судья – виртуальный аватар, за которым скрывается тот самый ИИ.

Согласно данным Европейской комиссии по вопросам правосудия (CEPEJ), в таких странах, как Франция, Великобритания и США, применяются системы искусственного интеллекта. Однако наблюдаются некоторые различия в сферах их использования. Во Франции ИИ-технологии задействованы исключительно в рамках гражданского судопроизводства, в то время как в Соединенных Штатах и Великобритании их применение распространяется и на уголовные дела, хотя и с определенной осторожностью. Так, в Великобритании ИИ-системы используются для прогнозирования, результаты которого учитываются судами при решении вопроса об освобождении подозреваемых под залог.

Большинство европейских государств пока отказываются от применения ИИ для принятия процессуальных решений, но активно используют такие технологии в сфере выявления и расследования преступлений. Например, система под названием "Connest" позволяет в кратчайшие сроки анализировать огромные массивы данных финансовых операций, что значительно повышает эффективность поиска. Кроме того, международная база данных о случаях сексуальной эксплуатации несовершеннолетних (ICSE DB) помогает идентифицировать как жертв, так и преступников посредством анализа визуальных и аудиоматериалов [14. С. 236].

Использование ИИ в качестве помощника может иметь значительный потенциал для уголовного процессуального права. Внедрение данной технологии может улучшить эффективность и прозрачность досудебной деятельности органов предварительного расследования и судебных процессов, минимизировать вероятность ошибок и предоставить независимую и объективную оценку доказательств.

В части использования технологий искусственного интеллекта в уголовном судопроизводстве примечательно, что в 2022 году Верховный суд Китая обязал судей консультироваться с ИИ по каждому делу, а при наличии отличий в итоговом решении с рекомендациями нейронной сети, судья обязан это обосновать. А в Шанхае на основе ИИ используется виртуальный прокурор, который может предъявить обвинение с точностью 97 процентов на основе устного описания судебного дела [5].

Внедрение методов ИИ в судебную систему КНР сократило среднюю рабочую нагрузку судей более чем на треть и сэкономило 1,7 млрд рабочих часов китайским жителям с 2019 по 2021 г., а также около 300 млрд юаней, сообщается в докладе Верховного народного суда КНР [2].

В США используется система DARE, которая отслеживает визуальные изменения мимики лица, голоса и речи человека и позволяет распознавать ложные показания в судебном процессе. В ряде штатов США используется алгоритм Recidivismmodels, который на основе статистических данных об осужденных создает прогноз совершения конкретным лицом рецидива, что используется судьями при выборе того или иного вида наказания [2].

Используемый в Германии проект Smart Sentencing (<https://legaltechcologne.de/smart-sentencing>) предлагает судье информацию о средних значениях по видам наказаний, с уже рассмотренными делами со схожими характеристиками за аналогичное преступление.

Вместе с тем, помимо положительных практик применения цифровых технологий, имеют место и случаи выявления неудачного применения таких технологий. Одна из программ, используемых в Соединенных Штатах для оценки риска рецидива среди преступников, – это COMPAS. Тем не менее анализ эффективности этой нейронной сети показал, что она значительно чаще, чем для других групп, указывала на возможный риск повторного преступления в отношении афроамериканцев. Хотя это можно было бы объяснить определенными социально-экономическими тенденциями в соответствующих группах. Исследования также выявили, что ИИ может определять человека как потенциального рецидивиста, даже если он никогда не был заключен под стражу, но ответил на вопросы в электронной форме определенным образом [6. С. 52–58].

Кроме этого, негативным опытом применения ИИ является случай, описанный во многих СМИ. Так, ученый из Института биологии внутренних вод имени И. Д. Папанина Российской академии наук А. Цветков провел 10 месяцев под стражей. Следственными органами он подозревался в совершении убийства двух человек в августе 2002 года. При этом основанием для подозрения ученого послужили данные системы на основе искусственного интеллекта, которая нашла 55-процентное совпадение между Цветковым и фотороботом, нарисованным свидетелем более двух десятилетий назад [1].

Следовательно, необходимо учитывать, что технологии ИИ в настоящее время еще в достаточной мере не изучены и, соответственно, использование тех или иных их возможностей – это дело ближайшего и последующего будущего.

Так, в России в 2024 году запланирован запуск сервиса “Правосудие онлайн”, который будет интегрирован с другими государственными информационными системами, что будет способствовать созданию единого цифрового пространства и упрощению сбора и проверки необходимых сведений и материалов [4]. Мы полагаем, что вполне возможно использование ИИ при анализе собираемых в ходе предварительного расследования доказательств или показаний в судебном разбирательстве, с целью выявления противоречий, несостыковок и иной информации, необходимой для установления истины по делу. Документально-технический, и процессуальный аспект собирания и оценки допустимости доказательств может быть усилен применением ИИ.

Вместе с тем имеются и мнения о возможности первого подхода использования ИИ [11. С. 190]. Для разрешения этого вопроса предлагаю рассмотреть достоинства и недостатки данных технологий с точки зрения их соответствия принципам уголовного процесса.

Так, несравненными достоинствами ИИ являются его точное следование букве закона, что соответствует принципу законности, изложенном в ст. 7 УПК РФ. Независимость от сторон процесса, беспристрастность, неподкупность, объективность – все это непосредственно относится к деятельности ИИ, что согласуется с принципом независимости судей, закрепленным в ст. 8.1 УПК РФ.

Вместе с тем главной проблемой использования ИИ при вынесении судебных решений является то, что он не несет и не может нести ответственности за свои результаты. А возложение ответственности на должностных лиц в уголовном процессе за совершенные ими действия является гарантом соблюдения данными лицами всей совокупности принципов уголовного процессуального права [9. С. 46].

Согласно ст. 17 УПК РФ, судья, присяжные заседатели, а также прокурор, следователь, дознаватель оценивают доказательства по своему внутреннему убеждению, основанному на совокупности имеющихся в уголовном деле доказательств, руководствуясь при этом законом и совестью, что является важным принципом уголовного процесса.

Как писал А. Ф. Кони: «Постановка звания судьи, пределы свободы его самостоятельности, обязательные правила его действий и нравственные требования, предъявляемые к нему, дают ясную картину состояния уголовного правосудия в известное время и в известном месте» [9. С. 71].

Следовательно, такие сугубо психологические свойства как внутреннее убеждение, совесть значительно сложнее программных алгоритмов ИИ, являются особенностью человека.

Также ИИ «недоступны аналогия закона и аналогия права, использование оценочных и ценностных критериев, закрепленных в законе, например, применение принципов справедливости и гуманизма при назначении наказания, соблюдение требований разумности и добросовестности» [10. С. 190]. Главным качеством человека является эмпатия – умение сочувствовать и сопереживать. Без него невозможно вынесение справедливых решений.

Если говорить о стабильности и объективности ИИ, стоит отметить, что при разработке (обучении) нейронной сети принимают участие конкретные люди, которые могут умышленно либо неосознанно влиять на определенные алгоритмы, в результате чего может проявляться субъективность в ряде критериев работы ИИ. Необходимо отметить, что использование искусственного интеллекта при принятии юридически значимых решений сопряжено с определенными рисками.

Поскольку ИИ базируется на статистических методах, существует вероятность, что он будет акцентировать внимание на отдельных характеристиках дела, которым, по его алгоритмам, отдается наибольший вес. Это может привести к нарушению принципа презумпции невиновности, когда система будет склоняться к обвинению подозреваемого лица. Таким образом, внедрение ИИ в юридическую сферу требует тщательной проработки механизмов контроля и обеспечения соответствия его выводов принципам справедливого правосудия [11. С. 190]. Человек свой «субъективизм» может преодолеть, в отличие от ИИ, в который изначально могли быть заложены элементы предвзятости.

В этой связи мы считаем актуальными и результаты опроса работников федеральных органов о границах использования ИИ [12. С. 1134–1143]. Так, в большинстве своем, респонденты скептически воспринимают рассуждения о расширении внедрения искусственного интеллекта в уголовно процессуальную деятельность. Возможен губительный результат и для самих сотрудников – наличие «умных технологий» приведет к атрофии интеллектуальных способностей работников правоохранительных органов и судебной системы, утрате опыта и существующих наработок, накопленных многими поколениями. Подобные последствия, например, описаны в рассказе Филипа Дика «Особое мнение» еще в 1956 году [8. С. 365].

Вместе с тем правовые основы использования ИИ в современной России находятся на этапе своего развития. Проникая в сферу уголовного судопроизводства, указанная технология обоснованно вызывает вопрос о допустимости ее использования при производстве следственных действий.

В этой связи примечательно, что президент Российской Федерации В.В. Путин в начале 2024 года направил поручение Верховному Суду Российской Федерации, Генеральной прокуратуре России, Следственному комитету Российской Федерации, МВД России и Минюсту России, в котором прямо указал о заинтересованности внедрения ИИ в уголовное процессуальное право, рекомендовал «проанализировать практику применения технологий искусственного интеллекта при расследовании преступлений и при необходимости представить предложения по ее совершенствованию»[3].

Заключение. В заключение необходимо отметить, что внедрение технологий ИИ в уголовном процессуальном праве процесс неизбежный, так как развитие права в целом и его институтов в частности обязаны идти в ногу со временем, с происходящими в жизни государства и мира переменами. В ближайшей перспективе ИИ видится как активный помощник участников уголовного процесса, который способен значительно сокращать и упрощать ряд процедурных вопросов.

Список литературы

1. «Если глаза, нос и рот в нужном месте»: как ИИ может отправить лютого за решетку. URL: <https://www.ntv.ru/novosti/2804097> (дата обращения: 9.08.2024).
2. Нейросети в судебной системе: китайский симбиоз и российская тоска. URL: <https://legalacademy.ru/sphere/post/neiroseti-v-sudebnoi-sisteme-kitaiskii-simbioz-i-rossiiskaya-toska> (дата обращения: 10.08.2024).
3. Перечень поручений по итогам конференции «Путешествие в мир искусственного интеллекта» (утв. Президентом РФ 17.01.2024 № Пр-83). – URL: https://www.consultant.ru/document/cons_doc_LAW_467464 (дата обращения: 12.08.2024).
4. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_335184 (дата обращения: 08.08.2024).

5. Шанхайский народный суд в КНР заявил, что разработал прокурора на основе искусственного интеллекта. URL: <https://rg.ru/2021/12/27/shanhajskij-narodnyj-sud-razrabotal-prokurora-na-osnove-ii.html> (дата обращения: 10.08.2024).
6. Амиянц К. А., Чемеринский К.В., Использование искусственного интеллекта в современной судебной системе и права человека // Международный журнал гуманитарных и естественных наук. 2019. № 11-3. С. 52–58.
7. Глимеда В. В. Перспективы и проблемы применения искусственного интеллекта в отечественном судопроизводстве // Современный ученый. 2020. № 6. С. 320–327.
8. Дик Ф. К. Особое мнение: рассказы: [пер. с англ.] // Филип Дик. СПб. : Амфора, 2004. С. 365.
9. Кони А. Ф. Нравственные начала в уголовном процессе (Общие черты судебной этики) // Юриспруденция. 2011. № 1. С. 71.
10. Лебедев З. С. Некоторые вопросы применения искусственного интеллекта в уголовном процессе России // Основы ЭУП. 2021. № 4. С. 46.
11. Момотов В. В. Искусственный интеллект в судопроизводстве: состояние, перспективы использования // Вестник Университета имени О. Е. Кутафина. 2021. № 5 (81). С. 190.
12. Никурадзе Н. О.; Мищенко, Е. В.; Марина, Е. А. Искусственный интеллект в уголовном процессе: перспективное будущее или утопия? // Журнал Сибирского федерального университета. Гуманитарные науки. 2024. №17 (6). С. 1134–1143.
13. Шаблова Е. Г., Правосудие и искусственный интеллект: перспективы и проблемы // Цивилистика: от прошлого к современности. 2022. С. 1367.
14. Kehl, Danielle, Priscilla Guo, and Samuel Kessler Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School. 2017. August. URL: <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041> (дата обращения: 03.08.2024).

В. А. Дударев,
старший преподаватель,
Брянский государственный университет
имени академика И. Г. Петровского

СОВРЕМЕННЫЕ ЦИФРОВЫЕ ТЕХНОЛОГИИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация. В статье рассматриваются перспективы внедрения цифровых технологий в сферу уголовного судопроизводства (в частности, в судебное и досудебное производство). Пристальное внимание уделено конкретным технологиям, которые уже активно используются в уголовном судопроизводстве, проведена их критическая оценка, а также очерчены законодательные перспективы внедрения иных инновационных технологий.

Ключевые слова: цифровизация, цифровые технологии, искусственный интеллект, нейросети, уголовное судопроизводство

MODERN DIGITAL TECHNOLOGIES IN CRIMINAL PROCEEDINGS

Abstract. The article discusses the prospects for the introduction of digital technologies in the field of criminal justice (in particular, in judicial and pre-trial proceedings). Close attention is paid to specific technologies that are already actively used in criminal proceedings, their critical assessment has been carried out, and legislative prospects for the introduction of other innovative technologies have been outlined.

Keywords: digitalization, digital technologies, artificial intelligence, neural networks, criminal proceedings

Введение. Наука, как и техника, – важные процессы развития человеческого общества, благодаря им появляются различные технологии, ускоряющие деятельность человека.

В XXI веке произошла 4-я промышленная революция, в которой особо внимание заслуживают Интернет, виртуальная реальность, 3D-печать, квантовые вычисления, искусственный интеллект, нейросети, метавселенные и т. п. Благодаря всем этим изменениям активно развиваются и цифровые технологии.

Следующим важным шагом в этом направлении стало проведение «Года науки и технологий – 2021», с инициативой которого выступил Президент РФ Владимир Путин. В течение года в разных регионах России было проведено более 5,5 тысяч соответствующих мероприятий. Затем президент подписал важнейший, на наш взгляд, указ о проведении в России десятилетия науки и технологий (2022–2031 гг.) [6], что говорит о важности дальнейшего развития этого направления.

Основная часть. Сегодня цифровые технологии активно внедряются и в российское уголовное судопроизводство, что отмечается уже многими авторами [9]. Однако это пока не тот уровень, чтобы говорить о полном переходе к высоким технологиям в отличие от остальных институтов российского общества, в которые цифровые технологии уже проникли. И если судебному производству уделено больше внимания в данном вопросе, то внедрение цифровых технологий в досудебное производство значительно отстает.

В 2024 году должен был заработать так называемый суперсервис «Правосудие онлайн», который позволит дистанционно, через портал Госуслуг участвовать в судебном процессе. Благодаря этой технологии будет возможна подача документов в суды всех уровней, ознакомление с материалами дела, присутствие на судебных заседаниях, а также получение судебных решений в личный кабинет.

Развитая цифровая инфраструктура страны позволяет решать важные задачи, одной из которых является быстрый доступ граждан к государственным услугам. Изучение вопросов цифровизации показало, что, благодаря внедрению цифровых технологий в различные сферы российского общества, происходит определенная положительная динамика в сторону автоматизации и упрощения многих процедур.

Проведенное нами эмпирическое исследование по вопросам цифровизации и цифровых технологий [1, 2] показало нам, как сегодня люди относятся к цифровым технологиям (рис. 1).

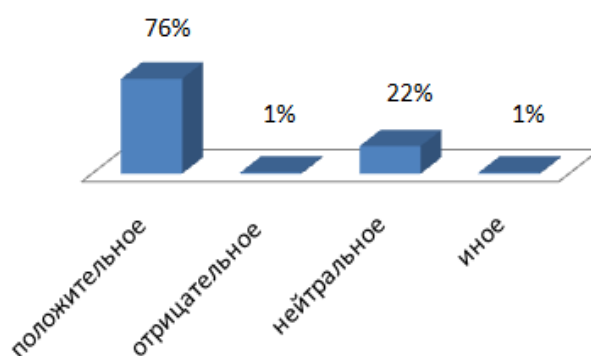


Рис. 1. Отношение к цифровым технологиям

Согласно результатам опроса, 76% респондентов выражают положительное отношение к цифровым технологиям, что подтверждает их позитивное влияние на различные аспекты нашей жизни. Однако 22% опрошенных занимают нейтральную позицию, считая, что технологии не приносят ни пользы, ни вреда, а 2% относятся к ним негативно.

На следующем этапе исследования мы получили ответ на другой значимый вопрос. Так, 85% участников считают, что цифровые технологии являются благом, тогда как 4% придерживаются противоположного мнения. Несмотря на явное преобладание положительных оценок, 11% респондентов выразили альтернативную точку зрения по данному вопросу (рис. 2).

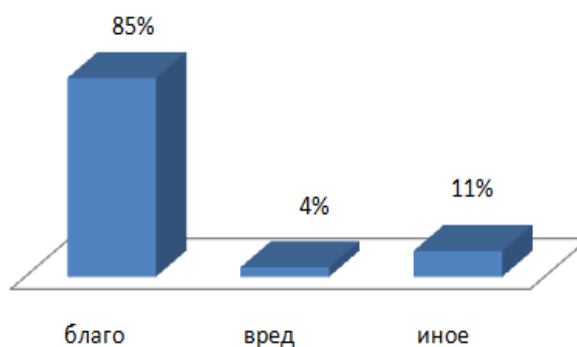


Рис. 2. Цифровые технологии

Заключение. Таким образом, в современном российском обществе уже не только внедрены различные цифровые технологии, но и активно используются [10]. Как преступники совершенствуют свои преступные действия и способы, используя современные технологии, так и уголовный процесс должен идти в ногу с развитием научно-технического прогресса, применяя новые цифровые технологии в борьбе с преступностью. Отмеченные нами лишь некоторые элементы

высоких технологий – это лишь начало большого и длинного пути развития цифровой трансформации всего уголовного судопроизводства.

Список литературы

1. Дударев В. А. Современные цифровые технологии и их влияние на несовершеннолетних // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 4. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 340 с. С. 192–202. DOI: http://dx.doi.org/10.21202/978-5-8399-0817-8_4_340
2. Дударев В. А. Внедрение цифровизации и цифровых технологий в современное российское общество // Современные технологии: актуальные вопросы теории и практики: сборник статей VI Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение», 2023. – С. 50–54.
3. Концепция информационной политики судебной системы на 2020 – 2030 годы (одобрена Советом судей РФ 05.12.2019) [Электронный ресурс] // СПС «Консультант Плюс».
4. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203 // Собрание законодательства Российской Федерации. – 2017. – № 20, ст. 2901.
5. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 № 490 // Собрание законодательства РФ. – 2019. – № 41, ст. 5700.
6. Об объявлении в Российской Федерации Десятилетия науки и технологий (вместе с «Положением о Координационном комитете по проведению в Российской Федерации Десятилетия науки и технологий»): Указ Президента РФ от 25.04.2022 № 231 // Собрание законодательства РФ. – 2022. – № 18, ст. 3052.
7. Федеральный закон от 25.12.2023 № 672-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» [Электронный ресурс] // СПС «Консультант Плюс».
8. «Это мой первый двойник». Путин задал вопрос Путину. URL: <https://www.fontanka.ru/2023/12/14/73018889/> (дата обращения: 28.08.2024).
9. Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. – 2023. – Т. 1, № 1(2). – С. 481–497. <https://doi.org/10.21202/jdtl.2023.20>. EDN: acsqxh.
10. Дмитриева А. А., Пастухов П. С. Концепция электронного доказательства в уголовном судопроизводстве // Journal of Digital Technologies and Law. – 2023. – Т. 1, № 1(1). – С. 270–295. <https://doi.org/10.21202/jdtl.2023.11>. EDN: SGAOKS.

Е. В. Ефимов,
кандидат технических наук,
Институт государства и права
Российской академии наук

СООТНОШЕНИЕ СРЕДСТВ ДОКАЗЫВАНИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ И РЕЗУЛЬТАТОВ РАБОТЫ АЛГОРИТМОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В развитие теории средств доказывания по С. Б. Россинскому впервые показано, что результаты работы систем искусственного интеллекта в процессе доказывания по уголовному делу являются вспомогательными средствами доказывания. Обосновано дополнение состава вспомогательных средств доказывания результатами работы алгоритмов искусственного интеллекта. Введен четвертый отличительный признак вспомогательных средств доказывания и на этом основании дано новое определение категории.

Ключевые слова: уголовное судопроизводство, доказательства, доказывание, средства доказывания, вспомогательные средства доказывания, налоговые преступления, искусственный интеллект, алгоритмы искусственного интеллекта, результаты работы алгоритмов искусственного интеллекта

CORRELATION OF MEANS OF PROOF IN CRIMINAL PROCEEDINGS AND THE RESULTS OF ARTIFICIAL INTELLIGENCE ALGORITHMS

Abstract. In the development of the theory of means of proof according to S.B. Rossinsky, it was shown for the first time that the results of the work of artificial intelligence systems in the process of proving a criminal case are auxiliary means of proof. The addition of the composition of the auxiliary means of proof by the results of the work of artificial intelligence algorithms is justified. A fourth distinctive feature of the auxiliary means of proof has been introduced and, on this basis, a new definition of the category has been given.

Keywords: criminal proceedings, evidence, proof, means of proof, auxiliary means of proof, tax crimes, artificial intelligence, artificial intelligence algorithms, results of artificial intelligence algorithms

Создание сложных по структуре и составу алгоритмов автоматизированного и автоматического сбора и обработки данных, представленных в самых разнообразных цифровых форматах, высокая скорость аналого-цифрового преобразования, увеличение производительности процессоров и объемов памяти с применением распределенной архитектуры компьютерных систем привели к качественному изменению их потребительских свойств. Программно-алгоритмические комплексы, реализуемые на компьютерных системах высокой производительности, обладают уникальными возможностями, что не без участия разработчиков привело к формированию новой терминологии понимания таких систем как систем искусственного интеллекта (СИИ). Многие исследователи прибегли к анализу возможностей СИИ в разрезе их применимости в уголовном судопроизводстве [1, 3, 4, 12, 14]. Перспективность роста производительности,

варианты технического совершенствования СИИ и расширения их возможностей не вызывают сомнения у процессуалистов, и не являются предметом исследования процессуальной науки. Вопрос заключается в том, что может дать СИИ процессу и в каком качестве это может быть использовано в уголовном судопроизводстве.

Так называемые системы искусственного интеллекта имеют структуру вычислительной системы. Процессинговая, обрабатывающая часть содержит компьютерную систему, обладающую универсальностью по отношению к реализуемым программам и собственно программный комплекс. Программный комплекс в свою очередь создан на базе алгоритмов. Вся специфика действия СИИ заложена именно в алгоритмах и их программной реализации. Свойства системы искусственного интеллекта полностью определяются возможностями программно-алгоритмического комплекса (ПАК ИИ). По сути, искусственный интеллект – это реализованный на компьютере развитый алгоритм, иначе – *всего лишь алгоритм* [3, с. 184], созданный человеком, и обладающий не только возможностями, но и ограничениями.

Анализ возможностей и ограничений ПАК ИИ применительно к уголовному процессу привел многих исследователей к закономерному выводу: с помощью математических алгоритмов с предустановленным описанием показателей и критериев качества по каждому из доказательств, определенных в ч. 2 ст. 74 УПК РФ, невозможно обеспечить исполнение уголовно-процессуального принципа свободы оценки доказательств. Таким образом, мечту фантастов – автоматизированное доказывание – обеспечить, по крайней мере, на данном этапе развития ПАК ИИ, невозможно.

Однако использовать результаты работы алгоритмов искусственного интеллекта в качестве вспомогательного средства доказывания возможно, и в некоторых случаях, особенно в информационно наполненных и сложных составах, таких, какие имеют место по налоговым преступлениям [13, с. 121], рационально.

Основой уголовного процесса является доказывание, что неоднократно отмечали признанные ученые-процессуалисты, называя доказывание «стержнем», «душой», «сердцевиной» уголовного судопроизводства [5, с. 82]. Доказывание осуществляется применением уголовно-процессуальных средств доказывания.

С.Б. Россинским в ряде работ [5–11], рассматриваемых совместно, обоснована теория средств доказывания, естественно отвечающая на все вопросы и вскрывающая все особенности, присущие категории «средства доказывания»: разграничены широкий и узкий подходы к пониманию термина, даны основы видовой классификации, введено определение, проанализированы отдельные виды. На указанной основе под *средствами уголовно-процессуального доказывания* будем понимать информационные объекты, прямо указанные в законе или обусловленные его смыслом, позволяющие субъектам уголовного судопроизводства устанавливать юридические факты по уголовному делу и обосновывать правоприменительные решения, а сторонам – обеспечивать мотивированное влияние на содержание и форму таких решений.

Средства доказывания подразделяются на субъективные и объективные; здесь выберем именно такой классификационный признак в качестве обобщающего классификационного признака верхнего уровня. Такое деление позволяет различать средства доказывания в виде материальных объектов и действий (процессы), присущих доказыванию и являющиеся его средствами.

Субъективные средства доказывания представлены возможностью человеческого разума осуществлять информационную обработку объективных данных, а также промежуточных результатов такой обработки. Пошаговый процесс обработки первичных данных и формирования итоговых знаний из первичных данных и промежуточных результатов обработки, описывается байесовским процессом обработки информации в динамических системах марковского типа. Содержание объективных средств доказывания выступают как априорные знания, а возможности человеческого разума [10. С. 18] – как функция правдоподобия, последовательное применение которой к априорным данным и промежуточным результатам обработки позволяет получить апостериорную информацию. На основании последней аргументируется правовая позиция стороны, которая располагает объективными средствами доказывания.

Объективные средства доказывания структурно включают: (1) собственно доказательства; (2) формальные средства доказывания; (3) вспомогательные средства доказывания.

К *собственно доказательствам* относятся так называемые «следовые» средства доказывания – прямо предусмотренные ч. 2 ст. 74 УПК РФ объекты информационного содержания, непосредственно в себе отразившие следы преступления. В процессе доказывания выявление действительных обстоятельств дела устанавливает истинность юридических фактов, составляющих предмет доказывания и проявившихся в момент совершения преступления, а также в прошлом и будущем относительно него [9. С. 30-32; 12. С. 91].

Формальные средства доказывания не являются следовыми, не несут свойства отражения материи по расследуемому преступлению – юридические факты по материальным основаниям этого вида средств доказывания установлены задолго до преступления и в обстоятельствах, не обязательно связанных с ним. К ним относятся вступившие в законную силу судебные акты, преюдиции, презумпции, юридические фикции, доказательственные субституции, объективно подтвержденные результаты научных исследований, иные общепризнанные факты, включенные в словари, энциклопедии и справочники. Аргументирование правовой позиции стороны с помощью формальных средств доказывания возможно на основании прямого указания в законе или судебном акте, общепризнанности, неоспоримости.

Вспомогательные средства доказывания по содержанию близки формальным средствам, но в отличие от последних их истинность не является доказанной однозначно – в этом они близки опровержимым презумпциям, но не обладают их силой и применяются не напрямую, а опосредовано, через участие в субъективном доказывании [7. С. 247]. Н. С. Расуловой и С. Б. Россинским предложено считать представляемые специалистом в соответствии с требованиями уголовно-процессуального закона данные справочно-вспомогательными и разграничить их от других средств доказывания [6. С. 16]. В исходных работах

этот вид средств доказывания назван указанными авторами «справочно-вспомогательным». Для выбора такого названия имеются некоторые основания: в криминалистике имеется аналог – «справочно-вспомогательные учеты», в до-революционном юридическом дискурсе иногда применялся термин «справочный свидетель» по отношению к сведущему лицу, и т. д. Однако у слова «справочник» имеется признанное лексическое толкование, относящее это слово к формальным средствам доказывания; нам представляется, что все «справочное» относится к формальному виду. Семантический анализ дает слову «вспомогательный» более подходящий смысл по отношению к сути рассматриваемого вида средств доказывания (предназначенный в помощь кому-л., чему-л., служащий для оказания помощи, поддержки; подсобный; дополнительный; не основной); указанное справедливо также и для тех расширений состава вспомогательных средств доказывания, которое предлагается в представляемой работе. Ниже будет показано, что вспомогательными данными являются результаты работы алгоритмов искусственного интеллекта.

К *вспомогательным средствам доказывания* будем относить сведения дополнительного характера, источниками которых являются сведущие лица или информационные системы, позволяющие восполнить пробелы понимания обстоятельств уголовного дела, выполнить дедуктивные рассуждения, способствующие правильной оценке доказательств, установлению фактов, содействующие субъектам доказывания в обосновании правоприменительного решения, а сторонам – в аргументации своих позиций по влиянию на такие решения [11. С. 69].

Так, заключению эксперта, которое имеет характер выводов, в процессе доказывания отведена практически безальтернативная роль ввиду отсутствия процессуально альтернативных средств (а в ситуациях, предусмотренных ст. 196 УПК РФ, назначение судебной экспертизы имеет императивные свойства): заключение специалиста носит ярко выраженный вспомогательный характер [6. С. 18], поэтому последнее следует отнести к вспомогательным средствам доказывания.

Именно доказывание будет являться тем процессом, на который смогут информационно оказывать влияние алгоритмы СИИ, если будет предусмотрено правильное процессуальное оформление результатов их работы. Поэтому искать роль и место результатам работы алгоритмов искусственного интеллекта следует в составе средств доказывания. Можно показать, что результаты работы искусственного интеллекта могут нести статус вспомогательных средств доказывания.

Прежде всего, искусственный интеллект носит ярко выраженный информационный характер. С помощью средств ИИ обрабатываются информационные данные, представленные в различной форме.

ИИ является алгоритмом обработки информации. Алгоритм систем ИИ имеет особенность – он обладает высокой сложностью и большим объемом. Однако все указанные особенности – сложность, объем – не исключают того факта, что ИИ есть программа, реализованная на компьютере. Ни элементы распределенности, ни нейроархитектура, ни сложность, ни элементы обучаемости не дают оснований придать исключительные свойства ПАК ИИ, соотносимые

с разумными действиями и уж тем более искать замену последним. Это просто большой компьютер с большими возможностями.

Компьютеры позволяют решать многие задачи, которые человеку не под силу. Объемное вычислительное моделирование, задачи большого порядка человеку либо не под силу, либо реализуемы за неприемлемо большое время. Информационная революция, о которой говорить начали задолго до текущего состояния вычислительной техники, привнесла возможность решать информационные задачи более эффективным способом, чем это делает невооруженный разум человека. Однако во всех нюансах применения компьютеров отчетливо проявляется вспомогательная роль, помогающая человеку решать отдельные информационные задачи.

У результатов работы ПАК ИИ внешний по отношению к субъектам доказывания и уголовному процессу в целом источник происхождения, и они передаются от технических средств субъектам доказывания в связи с консультацией, ответами на сложные или объемные вопросы по конкретному уголовному делу.

Результаты работы ПАК ИИ имеют не основное по отношению к процессу, а только вспомогательное предназначение. Они не подлежат обязательному использованию как средства уголовно процессуального доказывания, никакого аналога, например, ст. 196 УПК РФ по результатам ПАК ИИ не существует.

В-третьих, результаты ПАК ИИ не обязательно зависят от материальных следов-отображений, возникающих или изменяющихся под влиянием различных фрагментов окружающей реальности. Это не следовые средства доказывания. Конечно, с помощью алгоритмов ИИ могут быть исследованы следовые доказательства. Но это не означает, что результат такого исследования возможно использовать как следовое доказательство и только как его.

Заметим, что есть четвертая особенность. Это диалоговый характер использования вспомогательных средств. При их использовании всегда формируется некий вопрос, который задается исследователем [2. С. 30]. Без вопроса нет ответа, то есть нет самой информационной помощи, вспомоществования, потому что нет словесного объекта, по которому следует произвести информационную обработку, независимо от того, какой сложностью и объемом эта обработка должна удовлетворять и какие исходные данные должны быть использованы на входе в СИИ при производстве машинного анализа [3. С. 291].

Список литературы

1. Еремеев Д. В. Перспективы использования искусственного интеллекта в уголовном судопроизводстве // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. – 2022. – Т. 8 (74), № 1. – С. 141-148.
2. Зашляпин Л. А. Вопросы в допросе подсудимого по УПК РСФСР 1923 г. / Сибирские уголовно-процессуальные и криминалистические чтения. – 2023. – № 4. – С. 28–40. – DOI 10.17150/2411-6122.2023.4.28-40. – EDN LWAMCM.
3. Моисеев Н. Н. Математика ставит эксперимент. – М.: Наука, 1979. – 226 с.

4. Россинская Е. Р. Нейросети в судебной экспертологии и экспертной практике: проблемы и перспективы // Вестник Университета имени О. Е. Кутафина (МГЮА). 2024. № 3. С. 21–33.

5. Россинский С. Б. Доказывание по уголовному делу: познание или обоснование? // Законы России: опыт, анализ, практика. – 2020. – № 5. – С. 80–87.

6. Россинский С. Б., Расулова Н. С. Заключение эксперта и заключение специалиста как средства доказывания в уголовном судопроизводстве: каковы критерии их разграничения? // Вестник Уральского юридического института МВД России. – 2022. – № 2. – С. 15–20.

7. Россинский С. Б. О широком и узком подходах к пониманию средств доказывания в уголовном судопроизводстве // Вестник Восточно-Сибирского института МВД России. – 2023. – № 1(104). – С. 246–255.

8. Россинский С. Б. Размышления о сущности доказывания в уголовном судопроизводстве // Труды Института государства и права РАН. – 2022. – Т. 17, № 2. – С. 176–197.

9. Россинский С. Б. Субъективные средства доказывания в уголовном судопроизводстве // Юридическое образование и наука. – 2023. – № 2. – С. 29–34.

10. Россинский С. Б. Уголовно-процессуальное доказывание – совокупность познавательного-удостоверительных приемов и аргументационно-логических операций // Труды Академии управления МВД России. – 2023. – №1(65). – С. 16–22.

11. Россинский С. Б. Уголовно-процессуальная форма: сущность, проблемы, тенденции и перспективы развития // Актуальные проблемы российского права. – 2020. – № 9. – С. 67–79.

12. Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law – 2023. – № 1(2). – С. 481–497.

13. Шарипова А. Р. Процессуальные особенности уголовного преследования по делам о налоговых преступлениях. // Журнал российского права. 2024. – № 4. – С. 119–131.

14. Яшин С. Н., Иванов А. А., Иванова Н. Д. Анализ зарубежного опыта использования технологических платформ // Цифровая экономика и индустрия 4.0: Форсайт Россия: материалы науч.-практ. конф. с зарубежным участием, Санкт-Петербург, 26–28 марта 2020 г. – СПб.: ПОЛИТЕХ-ПРЕСС, 2020. – С. 121–123.

Л. В. Иванова,

кандидат юридических наук, доцент,
Тюменский государственный университет

ДИФФЕРЕНЦИАЦИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ В СФЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И РОБОТОТЕХНИКИ: ПОСТАНОВКА ПРОБЛЕМЫ

Аннотация. В статье рассматривается проблема определения виновного субъекта при причинении вреда умными роботами. Предлагается дифференцированный подход к закреплению ответственности в зависимости от степени ав-

тономности работа (полной или частичной) и в зависимости от осуществления роботом конкретного вида деятельности (совместно с человеком либо в его отсутствие).

Ключевые слова: ответственность, искусственный интеллект, робототехника, робот, субъект, дифференциация, уголовное право, цифровые технологии

Исследование выполнено за счет гранта Российского научного фонда № 24-28-01112, <https://rscf.ru/project/24-28-01112/>

DIFFERENTIATION OF CRIMINAL LIABILITY IN THE SPHERE OF ARTIFICIAL INTELLIGENCE AND ROBOTICS: STATEMENT OF THE PROBLEM

Abstract. The article examines the problem of determining the guilty subject when harm is caused by robots with artificial intelligence systems. It is noted that criminal legislation does not contain special crimes in the field of using robots or artificial intelligence technologies. The article proposes a differentiated approach to liability depending on the degree of autonomy of the robot (full or partial) and depending on the implementation of a specific type of activity by the robot (together with a person or in his absence).

Keywords: responsibility, artificial intelligence, robotics, robot, subject, differentiation, criminal law, digital technologies

The research was supported by the grant from the Russian Science Foundation, Project № 24-28-01112, <https://rscf.ru/project/24-28-01112/>

Цифровизация практически всех сфер жизни общества в настоящее время уже является привычным явлением. Но стремительное развитие цифровых технологий неизбежно поднимает вопросы безопасности, особенно если речь идет об автономных системах. Робототехника как наука и практика проектирования, производства и применения роботов и робототехнических устройств [1] выступает ключевой областью экономического роста, с государственной поддержкой исследований и разработок в национальных интересах во многих государствах [6. С. 2].

Проблемы определения виновного субъекта в сфере робототехники и искусственного интеллекта возникают в случае причинения вреда автономными системами, которые принимают решения о совершаемых действиях независимо от человека (хотя, безусловно, заложенный в них алгоритм создавался человеком). Исследователями предлагается несколько подходов к решению вопроса об ответственности роботов с системами искусственного интеллекта, так как в отношении таких роботов можно вести речь об автономности и самостоятельности принимаемых решений [6]:

- предлагается юридическое признание правосубъектности таких роботов;
- предлагается так называемая строгая ответственность, в соответствии с которой владелец, разработчик или оператор системы с искусственным интел-

лектом автоматически становится ответственным за любой ущерб, причиненный таким роботом, независимо от намерений;

– предлагается установление стандарта халатности для роботов с искусственным интеллектом, в соответствии с которым разработчики, владельцы или операторы привлекаются к ответственности, если они не предпримут разумных мер предосторожности, чтобы предотвратить причинение вреда;

– предлагается распространить на роботов с искусственным интеллектом положения законов об ответственности за качество продукции, то есть рассмотрение таких роботов как продуктов, подверженных дефектам или повышенной опасности.

Также к ответственности могут быть привлечены и третьи лица в случаях, когда роботы с искусственным интеллектом находятся под их управлением.

Рассматривая сферу робототехники в широком смысле, представляется возможным выделить две группы ситуаций причинения вреда: причинение вреда робототехническим устройством и причинение вреда роботом. При причинении вреда робототехническим устройством, вопрос об установлении виновного субъекта и привлечении его к ответственности, не вызывает затруднений, так как согласно нормативным правилам, данное устройство не обладает всеми признаками робота и, по сути, всегда подконтрольно человеку. Следовательно, виновным за вред, причиненный при использовании робототехнического устройства, всегда будет конкретный субъект – физическое лицо: или разработавшее соответствующий механизм, или его эксплуатирующее или осуществлявшее техническое обслуживание.

Следует отметить, что уголовное законодательство не содержит специальных составов преступлений в сфере применения роботов или технологий искусственного интеллекта.

При причинении вреда роботом представляется, что во многом решение вопроса об ответственности конкретного субъекта зависит от степени автономности робота и самостоятельности «принимаемых решений» в конкретных обстоятельствах. Ответственность в области робототехники может различаться в зависимости от уровня автономности робота (полной или частичной) и характера выполняемой им деятельности (в сотрудничестве с человеком или без него). Можно утверждать, что какое общество, такой и искусственный интеллект и на данном этапе развития общества только человек несет ответственность за сознательно совершаемые им деяния.

Список литературы

1. ГОСТ Р 60.0.0.4-2023/ИСО 8373:2021. Национальный стандарт Российской Федерации. Роботы и робототехнические устройства. Термины и определения (утв. и введен в действие Приказом Росстандарта от 20.04.2023 № 255-ст). – URL: <https://files.stroyinf.ru/Data/800/80030.pdf> (дата обращения: 07.09.2024).
2. Бегишев И. Р. Автономная робототехника в системе уголовно-правовых отношений: монография. М.: Блок-Принт, 2023. 160 с.
3. Дремлюга Р. И. Преступность 4.0 (киберпреступность: вчера, сегодня, завтра). М.: Инфотропик Медиа, 2024. 340 с.

4. Шутова А. А. Особенности квалификации преступлений, совершаемых лицами, использующими технологии искусственного интеллекта в здравоохранении // Lex Russica (Русский закон). – 2023. – Т. 76, № 12(205). – С. 113–123. – DOI 10.17803/1729-5920.2023.205.12.113-123. – EDN PQTEET.

5. Anderson G., Berleant D. (2014) Innovation Theory and the National Robotics Initiative Effort of the National Science Foundation // Journal of the Washington Academy of Sciences. 2014. № 100(1). P. 1-20.

6. Girme A., Bendale U.S., Gharde U. The Dark Side of AI: Autonomous Crimes by AI Robots and the Need for Legal Reform // Indian Journal of Law and Legal Research. 2024. № 5(6). 5204-5218.

А. В. Креховец,
кандидат юридических наук,
Нижегородская академия МВД России

ЗАРУБЕЖНЫЙ И РОССИЙСКИЙ ОПЫТ В УГОЛОВНО-ПРАВОВОЙ РЕГЛАМЕНТАЦИИ ОТВЕТСТВЕННОСТИ ЗА ТРЕШ-СТРИМЫ

Аннотация. В статье рассматриваются вопросы регламентации ответственности за публичную демонстрацию совершаемых преступных деяний с использованием информационно-телекоммуникационных технологий, в частности, с использованием социальных сетей, различных цифровых платформ и др. Анализируются мнения российских ученых, позиция российского законодателя в вопросе противодействия названным противоправным деяниям, а также опыт ряда зарубежных стран в данном вопросе.

Ключевые слова: треш-стримы, Интернет-преступность, прямая трансляция, криминализация, интернет-безопасность, социальные сети, цифровые платформы

FOREIGN AND RUSSIAN EXPERIENCE IN THE CRIMINAL LAW REGULATION OF LIABILITY FOR TRASH STREAMS

Abstract. The article discusses the issues of regulating responsibility for the public demonstration of criminal acts committed using information and telecommunications technologies, in particular, using social networks, various digital platforms, etc. The opinions of Russian scientists, as well as the Russian legislator on the issue of countering these illegal acts, as well as the experience of a number of foreign countries in this matter are analyzed.

Keywords: trash streams, Internet crime, live streaming, criminalization, Internet security, social networks, digital platforms

Введение. Возможность проведения прямых трансляций появилась несколько лет назад, однако за непродолжительное время данный инструмент приобрел серьезные масштабы. Более того, прямые трансляции стали чаще использоваться в негативном аспекте, в частности, для публичной демонстрации совершения преступлений. Не вызывает сомнений, что преступления, транслируе-

мые в прямом эфире, становятся все более распространенными по мере совершенствования технологий, в связи с чем вопрос надлежащего противодействия проведению треш-стримов приобретает особую актуальность.

Основная часть. Потенциальная и реальная общественная опасность таких деяний признается законодателями различных стран, и Российская Федерация в данном вопросе не является исключением. Уже долгое время вопрос уголовно-правовой оценки треш-стримов вызывает оживленные дискуссии в российских научных кругах. Анализ специальной литературы позволяет выделить несколько подходов к уголовно-правовой оценке треш-стримов.

Есть специалисты, по мнению которых оснований для внесения изменений в действующее российское уголовное законодательство нет. Данную точку зрения поддерживают, к примеру, Е. Н. Рахманова, А. Н. Берестовой, П. В. Цветков. По мнению авторов, действия треш-стримеров следует оценивать по соответствующим статьям УК РФ (причинение вреда здоровью, убийство и др.) в зависимости от выполняемой ими роли (организаторы, пособники и др.) [8, С. 137].

Некоторые зарубежные страны обратили внимание на необходимость противодействия треш-стримам несколько ранее, чем Российская Федерация. Проведенный анализ зарубежного опыта в разрешении вопроса о запрете треш-стримов свидетельствует о том, что зачастую данный вопрос является достаточно сложным с точки зрения его соотношения с конституционными положениями того или иного государства. Так, в Соединенных Штатах Америки (далее – США) вопрос о борьбе с треш-стримами поднимается чуть ли не ежегодно. Впервые необходимость противодействия треш-стримам на законодательном уровне была обозначена в 2017 году сенатором-республиканцем Ф. Бойлом. Законопроект Бойла предполагал умышленную видеозапись или помощь другому лицу в записи видео во время совершения тяжкого преступления относить к тяжкому преступлению класса Е.

В 2022 году после того, как вооруженный мужчина из огнестрельного оружия убил не менее десяти человек в одном из продуктовых магазинов в Нью-Йорке и транслировал происходящее на платформе Twitch, генеральным прокурором штата Летиции Джеймс был представлен доклад, ключевой идеей которого являлась необходимость криминализации создания видеозаписей или изображений убийства лицом, его совершившим. Впрочем, данное предложение так и не было принято. Первой поправкой Конституции США американским гражданам гарантируется право на свободу слова. Таким образом, проведение прямых трансляций оценивается как один из способов реализации данного права. Исключениями являются случаи распространения информации, содержащую в себе реальные угрозы, детскую порнографию, лжесвидетельство. Кроме того, раздел 230 Закона о благопристойности в сфере коммуникаций США предоставляет платформам иммунитет от привлечения их к ответственности за пользовательский контент, любого, в том числе непристойного содержания в том случае, если они не предпринимаяют разумные шаги для его удаления.

Интересный опыт в противодействии проведению треш-стримов имеет Новая Зеландия. В 2019 году Брентов Таррант вошел в мечеть Аль-Нур в Крайстчерче и убил 42 человека. Выйдя из мечети, он убил еще одного человека,

а затем продолжил свою серию убийств. В конечном счете убитыми оказались 49 человек. Совершаемые преступления Таррант транслировал в прямом эфире на Facebook⁶. Видео Тарранта было квалифицировано как преступление. Согласно положениям Закона о фильмах, видео и публикациях Новой Зеландии (1993 г.), хранение или распространение определенных видеоматериалов, наказывается штрафом в размере до 10 000 долларов, если лицо не знало, что они являются запрещенными, или тюремным заключением сроком до 14 лет, если оно знало, что данное действие является «предосудительным» [10].

Великобритания в вопросе противодействия распространению проведения треш-стримов в 2019 году выдвинула идею о возложении обязанностей по отслеживанию и удалению вредоносного контента на руководителей социальных сетей. В результате обсуждения в 2023 году был принят Закон о безопасности в Интернете, предусматривающий ряд новых обязанностей для руководителей социальных сетей и поисковых сервисов. В частности, данный Закон возложил на провайдеров новые обязанности по внедрению систем и процессов для снижения рисков использования их услуг в противоправных целях, а также по удалению противоправного контента в случае его появления.

В 2019 году Австралией был принят закон, также возложивший ответственность на компании социальных сетей за распространение контента, разжигающего ненависть, на своих платформах. Согласно принятому закону, любые формы медиа, изображающие терроризм, убийства, покушения на убийство, пытки, изнасилования и похищения, независимо от того, происходят ли они в Австралии или за ее пределами, считаются «отвратительным жестоким поведением» и должны быть удалены с платформ социальных сетей.

Заключение. Таким образом, результаты проведенного анализа подхода Российской Федерации, а также опыта ряда зарубежных стран в вопросе противодействия проведения треш-стримов свидетельствуют, что общественная опасность таких деяний признается на мировом уровне и требует особого внимания со стороны органов государственной власти.

Список литературы

1. Федеральный закон от 08.08.2024 № 218-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // «Собрание законодательства РФ», 12.08.2024, № 33 (Часть I), ст. 4914.
2. Адамов А. А. Уголовно-правовой анализ «треш-стримов»: особенности законодательной регламентации / А. А. Адамов, Д. А. Абуков // Тенденции развития науки и образования. – 2024. – № 105-6. – С. 13-17.
3. Арестов А. В. Треш-стримы – новое веяние кибер преступности, проблемы законодательного регулирования // Студент года 2022 : Сборник статей XXIII Международного научно-исследовательского конкурса, Пенза, 05 ноября 2022 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 148-150.

⁶ Социальная сеть признана экстремистской организацией и запрещена в РФ.

4. Берестовой А. Н. Вопросы криминализации девиантного поведения в сети Интернет (уголовно-правовой аспект) // Юрист-Правоведъ. – 2023. – № 4(107). – С. 96-101.

5. Грачева Ю. В. Треш-стрим: социальная обусловленность криминализации / Ю. В. Грачева, С. В. Маликов // Актуальные проблемы российского права. – 2021. – Т. 16, № 6(127). – С. 202-210.

6. Григорьев В. Н. Об усилении уголовной ответственности создателей треш-стримов / В. Н. Григорьев, А. Ю. Терехов // Вестник Волгоградской академии МВД России. – 2021. – № 2(57). – С. 36-40.

7. Жаров К. А. Треш-стримы: уголовно-правовой аспект // Современный ученый. – 2023. – № 6. – С. 298-303.

8. Рахманова Е. Н. Треш-стрим – форма сетевой агрессии: уголовно-правовой анализ / Е. Н. Рахманова, А. Н. Берестовой, П. В. Цветков // Вестник Санкт-Петербургского университета МВД России. – 2023. – № 1(97). – С. 137-143.

9. Фильченко А. П. Охрана общественной нравственности от посягательств в форме прямых трансляций противоправного поведения (треш-стримов) // Труды Академии управления МВД России. – 2021. – № 4(60). – С. 90-100.

10. MACKLIN G. The Christchurch Attacks: Livestream Terror in the Viral Video Age. JULY 2019, VOLUME 12, ISSUE 6. [Электронный ресурс]. – URL: <https://etc.westpoint.edu/christchurch-attacks-livestream-terror-viral-video-age> (дата обращения: 05.01.2021).

А. К. Кукеев,
аспирант,

Омский государственный университет имени Ф. М. Достоевского

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИХ РОЛЬ В ПОВЫШЕНИИ ПРОЗРАЧНОСТИ И ЭФФЕКТИВНОСТИ АНТИКОРРУПЦИОННЫХ МЕРОПРИЯТИЙ

Аннотация. В данной статье рассматривается значение и влияние цифровых технологий на эффективность антикоррупционных мер. В работе анализируются различные инструменты и методы, используемые в борьбе с коррупцией. Цифровые технологии играют ключевую роль в повышении эффективности антикоррупционных мер. Они способствуют повышению прозрачности, снижению уровня коррупции и повышению доверия граждан к государственным институтам. Социальные сети и специализированные платформы общественного мониторинга предоставляют гражданам инструменты для уведомления о случаях коррупции и обсуждения вопросов прозрачности. К активным антикоррупционным мерам следует отнести роль общественного контроля в общественной жизни, ведь содействие активному участию общественности в антикоррупционных мероприятиях; электронные платформы для регистрации предприятий, получение лицензий в ведении финансово-хозяйственной, уплаты налогов и другие действия; уменьшение коммуникации между гражданами и государственными служащими для уменьшения коррупционных рисков. Использование цифровых ин-

формационных технологий для противодействия коррупции показало, что применение компьютерных автоматизированных программных средств и алгоритмов искусственного интеллекта является наиболее эффективным инструментом упрощения административных процессов, контроля прозрачности деятельности компании, органов власти.

Ключевые слова: коррупционные риски, искусственный интеллект, противодействие и борьба с коррупцией, цифровые платформы, мониторинг и анализ, цифровизация

DIGITAL TECHNOLOGIES AND THEIR ROLE IN INCREASING THE TRANSPARENCY AND EFFECTIVENESS OF ANTI-CORRUPTION MEASURES

Abstract. This article examines the importance and influence of digital technologies on the effectiveness of anti-corruption measures. Digital technologies play a key role in increasing the effectiveness of anti-corruption measures. They contribute to increasing transparency, reducing the level of corruption, and increasing citizens' trust in state institutions. Social networks and specialized public monitoring platforms provide citizens with tools for reporting corruption cases and discussing transparency issues. Active anti-corruption measures should include the role of public control in public life, because it promotes active public participation in anti-corruption measures; electronic platforms for registering enterprises, obtaining licenses in financial and economic management, paying taxes and other activities; reducing communication between citizens and government officials to reduce corruption risks. The use of digital information technologies to combat corruption has shown that the use of computer automated software and artificial intelligence algorithms is the most effective tool for simplifying administrative processes, controlling the transparency of the company's activities, and government bodies.

Keywords: corruption risks, artificial intelligence, counteraction and fight against corruption, digital platforms, monitoring and analysis, digitization

Введение. Коррупция стала одной из самых серьезных проблем современного общества [11]. Коррупция сдерживает экономическое развитие государства и делает невозможным установить надлежащий уровень развития страны в соответствии с международными стандартами. Соответственно, важно внедрять различные антикоррупционные меры, особенно в условиях развития цифровых технологий [10]. Снижение уровня коррупции – важный шаг на пути к устойчивому развитию общества [1. С. 6].

Основная часть. Одним из индикаторов 16 целей устойчивого развития (мир, справедливость и сильные институты) Организации Объединенных Наций (далее – ООН) является сокращение уровня коррупции [2]. Таким образом, даже на глобальном уровне нет задачи по искоренению коррупции. Это свидетельствует о рациональности и осознании задач и потребностей.

В свете усовершенствования антикоррупционных мер важным шагом стало утверждение Концепции антикоррупционной политики Республики Казахстан на 2022–2026 годы [3]. Новейшие технологии могут служить отличным рычагом для трансформации действий общества в борьбе с коррупцией из-за безбумаж-

ной среды, уменьшения бюрократии и освещения серых зон, где процветает коррупция [4].

Итак, мы убеждены, что подобный шаг вполне оправдан, поскольку цифровая трансформация может способствовать противодействию коррупции. Это возможно благодаря внедрению эффективных цифровых технологий и инноваций в сферу управления, финансов, администрирования и отчетности. Цифровые инструменты позволяют создать прозрачные и эффективные системы контроля, мониторинга и анализа деятельности, усложняющие возможность коррупционных действий. Электронное управление и отчетность обеспечивают уменьшение возможностей для совершения коррупционных схем и улучшают доступ к информации для общественности и контролирующих органов. Таким образом, цифровые технологии играют ключевую роль в повышении эффективности антикоррупционных мер. Они способствуют повышению прозрачности, снижению уровня коррупции и повышению доверия граждан к государственным институтам. В целях достижения максимальных результатов в части применения антикоррупционных мер необходимо комплексно решать указанную проблему и формировать отдельное стратегическое видение по этому вопросу.

Антикоррупционные меры предусматривают действия, направленные на противодействие и предотвращение коррупционных действий в различных сферах общественной жизни. Такие меры связаны с необходимостью реформирования законодательства и системной адаптации правовых норм к вызовам настоящего. В свою очередь, механизм реализации – это надлежащее функционирование антикоррупционных органов, которые совершают действия по досудебному расследованию, судебному производству, преследованию лиц, совершающих коррупционные деяния.

Цифровизация правительства способствует использованию информационных технологий в сфере предоставления государственных услуг. К таким возможностям можно отнести электронные платформы для регистрации предприятий, получения лицензий в ведении финансово-хозяйственной деятельности, уплаты налогов и других платежей, оплаты государственных услуг в различных сферах. При использовании информационных ресурсов отсутствует коммуникация между гражданами и государственными служащими и, как следствие, уменьшается вероятность коррупционных действий.

Существует достаточно много ресурсов, с помощью которых возможно получение важной информации: Верховным судом РК создан ряд информационных систем и сервисов: система «Төрелік», интернет-портал судебных органов, сервис «Судебный кабинет», электронные системы рассылки и другие. Внедряются элементы искусственного интеллекта, применяемые в сервисе «Цифровая аналитика судебной практики» [3, 5].

Ярким примером внедрения электронных систем и платформ для обеспечения прозрачности и конкуренции в процессе государственных закупок с целью предотвращения коррупции и злоупотреблений является платформа Единая платформа закупок. Информационные системы, такие как системы мониторинга и контроля государственных закупок, позволяют автоматизировать процессы проверки и обеспечивать выявление аномалий. К примеру, системы автоматиче-

ского анализа контрактов могут выявлять подозрительные соглашения и предупреждать о возможных коррупционных рисках.

Единая платформа закупок представляет собой электронную систему государственных закупок, целью которой является проведение процедуры государственных закупок максимально эффективно и прозрачно. Участники тендерной процедуры имеют доступ к самому тендеру, предложениям участников и результатам проведения. Все это проходит в режиме реального времени, расширяя доступ бизнеса к выходу на рынок услуг.

Благодаря автоматизации процессов и уменьшению бюрократических помех Единая платформа закупок помогает снизить расходы как для органов государственной власти, так и для поставщиков, а также способствует экономии бюджетных средств. Единая платформа закупок постоянно совершенствуется и адаптируется к современным требованиям, внедряя новые технологии и инструменты для улучшения процесса закупок.

Цифровая трансформация детерминирует: а) преобразование, изменение определенных явлений или процессов с нецифрового в цифровой формат; б) создание определенных явлений или осуществление процессов на основе цифровых коммуникаций и медиа инфраструктуры [7. С. 39].

В свою очередь, использование цифровых информационных технологий для противодействия коррупции показало, что применение компьютерных автоматизированных программных средств и алгоритмов искусственного интеллекта является наиболее эффективным инструментом упрощения административных процессов, контроля прозрачности деятельности компании, органов власти. Искусственный интеллект устраняет человеческий фактор в процессах принятия решений и способен отследить угрозу правонарушений без вмешательства человека [6, 8].

Цифровизация реальной правовой действительности способствует формированию новых цивилизационных явлений и процессов, возникновению нового правопонимания, мировоззрения и правовой культуры. Цифровая реальность выдвигает требования к юридической науке и практики, связанные с усовершенствованием механизмов правового регулирования различных сфер жизни основе современных цифровых технологий. Должен быть разработан механизм, обеспечивающий своевременное применение таких норм.

Поскольку электронное управление связано с деятельностью органов государственной власти и органов местного самоуправления с использованием информационно-телекоммуникационных технологий.

Цифровизация помогает функционировать таким инструментам, в которых сообщается о возможных фактах коррупционных или связанных с коррупцией правонарушений, других нарушений Закона РК «О противодействии коррупции», как анонимный канал связи. К анонимным каналам связи следует отнести: канал получения сообщений с использованием официального веб-сайта учреждения; канал получения сообщений с использованием электронных почтовых ящиков; канал получения голосовых сообщений с использованием технологии IP-телефонии (анонимная горячая линия); канал получения голосовых сообщений с использованием телефонной сети общего использования (анонимная горячая линия) [9].

Социальные сети и специализированные платформы общественного мониторинга предоставляют гражданам инструменты для сообщения о случаях коррупции и обсуждения вопросов прозрачности.

Среди непосредственных недостатков электронизации государственного механизма можно назвать наличие программных ошибок, сбоев, отсутствие понимания программой ситуации, отсутствие в программе эмпатии, потенциальные умышленные действия разработчиков программного обеспечения. Проблема противодействия коррупционным рискам, которые несут в себе новые информационные технологии, – это концептуальная проблема системного характера, которая влечет за собой настоятельную потребность пересмотра существующего механизма законотворчества.

Заключение. Важно четко понимать, какое деяние коррупционно, а какое нет, и соответственно установить суровое наказание за коррупционные преступления. Именно антикоррупционные органы способны проводить расследование и судебное разбирательство, мониторинг ситуации с коррупцией. Важно привлечение общественности и негосударственных организаций для мониторинга и контроля за деятельностью государственных институций.

Список литературы

1. Mugellini G., Villeneuve J.-P. Monitoring the Risk of Corruption at International Level: The Case of the United Nations Sustainable Development Goals. *European Journal of Risk Regulation*. 2019. № 10 (1). P. 1–7. DOI: 10.1017/err.2019.16
2. THE 17 GOALS. *United Nations*: website. URL: <https://sdgs.un.org/goals>
3. Коваль В. Д. Противодействие коррупции в таможенных органах в системе общегосударственных мер противодействия коррупции: Международно-правовой аспект // Вопросы российского и международного права. – 2018. – Т. 8, № 11А. – С. 70–76.
4. Sadok H. Fight Against Corruption Through Technology. *Advances in finance, a counting, and economics book series*. 2023. DOI: <https://doi.org/10.4018/978-1-6684-5007-9.ch013>
5. О применении информационных технологий в судопроизводстве. [Электронный ресурс]. URL: <https://sud.gov.kz/rus/content/cifrovizaciya> (дата обращения: 20.08.2024).
6. Кабылдин А. ИТ-технологии в противодействии коррупции: факторы успеха и риски неудачи // Государственное управление и государственная служба. 2023. № 2 (85). С. 32–43.
7. Утаров Е. Н. Цифровое реформирование деятельности Национального агентства по предотвращению коррупции // Закон и время. 2023. № 8. С. 37–42.
8. Шайменова А. Т. Практика использования цифровых технологий и искусственного интеллекта для борьбы с коррупцией // Фемида. 2022. № 2. С. 59–66.
9. О противодействии коррупции: Закон Республики Казахстан от 18 ноября 2015 года № 410-V ЗРК [Электронный ресурс]. URL: <https://adilet.zan.kz/rus/docs/Z1500000410> (дата обращения: 20.08.2024).
10. Противодействие коррупции и процессы цифровизации: научно-практическое пособие / Ю. В. Трунцевский, А. М. Цирин, Е. В. Черепанова и др.;

Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. М.: Инфотропик Медиа, 2023.

11. Противодействие коррупции: новые вызовы: монография / С. Б. Иванов, Т. Я. Хабриева, Ю. А. Чиханчин [и др.]; отв. ред. Т. Я. Хабриева. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М, 2018.

Э. Ю. Латыпова,
кандидат юридических наук, доцент,
заведующий кафедрой,
Казанский инновационный университет имени В. Г. Тимирязова,
Р. Р. Мусина,
старший преподаватель,
Казанский инновационный университет имени В. Г. Тимирязова,

О НОВОМ КВАЛИФИЦИРУЮЩЕМ ПРИЗНАКЕ В ОСОБЕННОЙ ЧАСТИ УК РФ – ПУБЛИЧНОЙ ДЕМОНСТРАЦИИ ПОСРЕДСТВОМ СМИ

Аннотация. Федеральным законом от 8 августа 2024 г. № 218-ФЗ в Уголовный кодекс РФ были внесены очередные изменения. В этот раз изменения охватывали ряд статей Особенной части УК РФ, а также ст. 63 УК РФ, в которую было внесено новоеотягчающее уголовную ответственность обстоятельство – п. «т», «совершение умышленного преступления с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»)». Необходимость внесения подобного рода дополнений в уголовное законодательство назрела достаточно давно, в связи с чем необходимо произвести определенное значение данных редакционных поправок.

Ключевые слова: средства массовой информации; СМИ; квалифицирующий признак преступления; публично демонстрирующееся произведение; публичная демонстрация; информационно-коммуникационные сети; компьютерные игры

ABOUT A NEW QUALIFYING FEATURE IN A SPECIAL PART OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION – PUBLIC DEMONSTRATION THROUGH THE MEDIA

Abstract. Federal Law No. 218-FZ of August 8, 2024 further amendments were made to the Criminal Code of the Russian Federation. This time, the changes covered a number of articles of the Special Part of the Criminal Code of the Russian Federation, as well as a new aggravating circumstance was introduced in Article 63 of the Criminal Code of the Russian Federation – paragraph "t", "committing an intentional crime with a public demonstration, including in the media or information and telecommunication networks (including the Internet)". The need to make such

additions to the criminal legislation has been overdue for a long time, and therefore it is necessary to make a certain value of these editorial amendments.

Keywords: mass media; mass media; qualifying sign of a crime; publicly displayed work; public demonstration; information and communication networks; computer games

Цифровизация и порождаемые ею процессы оказывают колоссальное влияние на окружающую нас действительность, в том числе влияя на правовую систему, что отмечается многими авторами [11]. В последние годы в Российской Федерации наблюдается повышенное внимание к обсуждению правовых аспектов новых явлений, обусловленных развитием социальных сетей [8]. Среди таких явлений – активное распространение так называемых треш-стримов, в ходе которых участники либо сами выполняют любые желания своих подписчиков, которые могут наблюдать происходящее в прямом эфире, либо совершают разнообразные действия, зачастую противоправного характера, в отношении других «очных» участников. Причем подобные действия совершаются с видимого одобрения участников, более того, могут являться способом их заработка, так как зрители могут переводить участникам так называемые «донаты», то есть вознаграждение. Причем, если первоначально стримы имели положительное наполнение, так как участники соревновались в своих умениях и навыках, например, устраивали различного рода разговорные или песенные баттлы (состязания), то в дальнейшем, в погоне за «легкими деньгами», в стримах стали устраивать издевательство над отдельными участниками, причиняли вред здоровью, совершали сексуальное насилие и даже причиняли смерть.

В то же время треш-стримы являются совершенно новой криминологической проблемой [2], и тем самым требуют проведения научного анализа.

Изначально стрим касался сетевых игр, и стример, то есть человек, ведущий трансляцию в Интернете, показывал в прямом эфире некоторые особенности («фишки») управления персонажем или прохождения сложных уровней в компьютерной игре. Таким образом, с одной стороны, стример обучает зрителей управлению игровым персонажем или особенностям игровой местности, а с другой – дает возможность ознакомиться с новой компьютерной игрой тем, у кого нет возможности ее приобрести (так как новые игры могут стоить довольно дорого) или не хватает мощности компьютера для самостоятельного использования в конкретной игре [4. с. 295].

Само понятие «треш-стрим», или «трэш-стрим», стало применяться на территории стран СНГ с 2010 года. Считается, что один из первых треш-стримов был организован Кириллом Зыряновым (VJLink), который вел трансляции по игре Dota2, но особого успеха не имел до тех пор, пока один из зрителей не выбил ему зубы прямо в эфире, после чего просмотры резко пошли вверх.

Нужно учитывать, что в стриме денежные средства получают как за сам факт просмотра предлагаемого контента на канале, так и за счет просмотра рекламы подписчиками, наличия возможной платной подписки, также за счет индивидуального вознаграждения – доната. Соответственно, чем больше подписчиков на канале и чем больше донатов – тем богаче стример. Доходы наиболее крупных и известных стримеров могут достигать нескольких миллионов в дол-

ларовом эквиваленте (при наличии нескольких миллионов подписчиков). В то же время стример несет и достаточно большие расходы, но их анализ выходит за рамки нашего исследования.

Полагаем, что проведение треш-стримов посягает на морально-нравственное состояние лиц, которые их просматривают [5. С. 97], а тем более – являются постоянными подписчиками, что также может негативно повлиять и на психическое состояние таких лиц, особенно если их психика является неустойчивой. Треш-стримы негативно влияют на их психологическое развитие подростков [6. С. 183], так как зачастую у несовершеннолетних возникает желание повторить аналогичные действия в прямом эфире [7. С. 794] (о чем свидетельствуют достаточно распространенные видео, где подростки нападают на одного из них, публично унижают, заставляют совершать определенные действия, причиняют вред здоровью и параллельно снимают указанные действия на телефон и выкладывают в своих социальных сетях.

С одной стороны, наличие видеозаписей или запись прямого эфира позволяет привлечь виновных лиц к ответственности [9. С. 112] (в том числе и уголовной в случае, если участники достигли возраста уголовной ответственности), и, с другой стороны, является доказательством того, что воспитанию подростков родители и школа уделяют чрезвычайно мало внимания.

В некоторых случаях треш-стримы совмещаются с иными мероприятиями развлекательного характера, например, с треш-квестами (аналог комнаты страха, но при этом участника могут избить или иным образом причинить вред здоровью) [10. С. 315]. При этом видеозапись треш-квеста может транслироваться в Интернет.

Можно согласиться с законодателем, что широкое распространение треш-стримов имеет серьезную общественную опасность, так как лица, их просматривающие, могут в дальнейшем сами совершать деяния аналогичного характера (но уже без видеозаписи), либо сам просмотр жестокого видео может негативно влиять на психику несовершеннолетних (которые нередко являются потребителями данного контента), так и лиц с неустойчивой психикой.

Список литературы

1. «О внесении изменений в Уголовный кодекс Российской Федерации» [Электронный ресурс]. URL: <https://base.garant.ru/409492465/>
2. Смирнов А. М. «Треш-стримы» как новая криминологическая проблема современности // Дневник науки. 2021. № 5 (53).
3. Латыпова Э. Ю. Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Oeconomia et Jus. 2019. № 2. С. 35 – 45.
4. Гильманов Т. Э., Гордеев М. А. Способы использования мошенниками бесплатных скриптов для компьютерных игр / Казанские научные чтения студентов и аспирантов имени В.Г. Тимирязова – 2022: материалы XII Международной научно-практической конференции студентов и аспирантов, 16.12.2022. В 3 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 480 с. С. 295–296.

5. Латыпова Э. Ю., Гильманов Э. М., Абдуллина А. Е., Гильманов Р. Э. Влияние нравственно-моральных норм на содержание уголовно-правовых норм в Уголовном кодексе России // Вестник экономики, права и социологии. 2022. № 1. С. 93-99.

6. Гильманов Э. М. Дигтерство и сталкерство как формы противоправного и опасного поведения несовершеннолетних // Социально-правовая защита детства как приоритетное направление современной политики: сборник материалов Международной научно-практической конференции. Чебоксары, 2018. С. 180 – 185.

7. Гильманов Э. М. Противодействие противоправным и опасным формам поведения несовершеннолетних // Достижения, проблемы и перспективы развития нефтегазовой отрасли: материалы Международной научно-практической конференции. Альметьевск, 2018. С. 792–795.

8. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.

9. Латыпова Э. Ю., Гильманов Р. Э., Бадрутдинов Р. Р. Роль правоохранительных органов и специальных служб в борьбе с преступлениями, совершаемыми в сфере компьютерных игр, и технические решения для их предотвращения // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 109–114. DOI: 696X-2024-39-4-109-114

10. Латыпова Э. Ю. Уголовная ответственность за нарушение безопасности проведения досуга в формате квеста // Правовое регулирование культурно-досуговых отношений и спортивной деятельности в контексте общественных и нравственных ценностей: современное состояние и мировые тенденции: сборник материалов Международной научно-практической конференции. Чебоксары, 2019. – С. 314–319.

11. Асли М. Р. Цифровые тренды криминологии и уголовного правосудия XXI века // Journal of Digital Technologies and Law. 2023. Т. 1, № 1(1). С. 235–250. <https://doi.org/10.21202/jdtl.2023.9>. EDN: ZMIRLT.

Э. Ю. Латыпова,
кандидат юридических наук, доцент,
заведующий кафедрой,
Казанский инновационный университет имени В. Г. Тимирязова,
К. М. Рогова,
магистрант
Казанский инновационный университет имени В. Г. Тимирязова

О ПРОЦЕССЕ ПРИЗНАНИЯ ЛИЦА ИНОСТРАННЫМ АГЕНТОМ

Аннотация. Приоритетными задачами любого государства являются поддержание безопасности, суверенитета и защита национальных интересов, но изменение внутривнутриполитической и внешнеполитической ситуации, а также развитие информационных технологий вызывают потребность в усовершенствовании имеющихся, и разработке новых механизмов реагирования на потенциальные угрозы. Одной из проблем, связанных с вопросами национальной безопасности, является возможность пребывания внутри страны лица, которое действует в ин-

тересах иного (иностранного) государства или таковой организации, – данное лицо признается иностранным агентом. Признание и установление статуса иноагента имеет важное значение для государства, так как таким образом открываются возможности для принятия эффективных мер по предотвращению, пресечению и нейтрализации действий, которые угрожают интересам и безопасности государства. Соответственно, необходимо исследовать процедуру признания лица иноагентом.

Ключевые слова: иностранный агент; иноагент; последствия признания иноагентом; организация, признанная иностранным агентом

ABOUT THE PROCESS OF RECOGNIZING A PERSON AS A FOREIGN AGENT

Abstract. The priority tasks of any state are to maintain security, sovereignty and protect national interests, but changes in the domestic and foreign policy situation, as well as the development of information technologies, cause the need to improve existing and develop new mechanisms to respond to potential threats. One of the urgent problems related to national security issues is the possibility of a person staying inside the country who acts in the interests of another (foreign) state or such an organization, this person is recognized as a foreign agent. Recognition and establishment of the status of a foreign agent is important for the State, as this opens up opportunities for taking effective measures to prevent, suppress and neutralize actions that threaten the interests and security of the State. Accordingly, it is necessary to investigate the procedure for recognizing a person as a foreign agent.

Keywords: a foreign agent; a foreign agent; the consequences of recognition as a foreign agent; an organization recognized as a foreign agent

Введение. В 2022 году были признаны иноагентами 188 человек, что почти в 2 раза больше, чем в 2021 году, когда их было всего 108 [1]. По данным Минюста РФ на август 2024 г., в России действовали 569 иноагентов, тогда как в соответствующем реестре числилось 763 иноагента [2]. Соответственно, одной из актуальных проблем является анализ положений правоприменительной практики, касающейся данной категории лиц.

Введение понятия «иностранный агент» в России имеет глубокую социально-историческую обусловленность. Раскрывая данное понятие, следует отметить, что в соответствии с законодательством Российской Федерации, а именно Федеральным законом от 14.07.2022 № 225-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием», «иностранным агентом признается лицо, которое получило или получает поддержку от иностранных организаций, а также находится под иностранным влиянием и осуществляет определенные, установленные данным законом виды деятельности» [3].

Основная часть. Термин «иноагент» был введен в 2012 году, с момента вступления в силу Федерального закона № 121-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента», где указывалось, что иностранным агентом признается «любая российская некоммерческая организация, кроме политических партий, кото-

рая получает финансирование (в виде денежных средств или любого другого имущества) от иных государств, а так же международных и зарубежных организаций, в том числе иностранных граждан»[4]. Но при этом данное лицо должно участвовать в политической деятельности на территории России и представлять интересы иностранных государств. Необходимо отметить, что в данном законодательном акте был определен порядок исключения иностранных некоммерческих организаций из реестра иноагентов:

- отсутствие полного и частичного финансирования зарубежных источников на срок, превышающий двенадцать месяцев;
- не ведение политической деятельности в течение трех лет.

Так, в соответствии со ст. 2 данного Федерального закона под иностранным влиянием понимается предоставление иностранным источником лицу поддержки и (или) оказание воздействия на лицо, в том числе путем принуждения, убеждения и (или) иными способами.

Признание лица иноагентом на территории России является сложной правовой процедурой, которая определяет статус и правовые обязанности таких лиц перед государством. В соответствии с Федеральным законом от 12 января 1996 года № 7-ФЗ «О некоммерческих организациях» [5] закрепляется ряд обязательных условий, при которых лицо может быть признано иностранным агентом.

Получившее статус иноагента лицо обязано пройти регистрацию в специальном реестре, который подконтролен Министерству юстиции Российской Федерации, после чего у таких лиц появляются дополнительные отчетные обязательства по предоставлению информации о своей деятельности и путях финансирования [6. С. 615].

Таким образом, делая вывод из всего вышесказанного, хотелось бы отметить, что иностранным агентом на территории Российской Федерации признается лицо, действующее в интересах иностранного государства и систематически получающее от такового имущество (в денежном или ином эквиваленте). Условиями признания лица иноагентом являются: наличие иностранного финансирования, участие в политической деятельности, наличие некоммерческой организации иностранного агента.

Процесс признания лица иностранным агентом включает следующие шаги.

Первоначальным этапом данной процедуры является сбор сведений, данных деятельности, а также полный анализ таковой деятельности лица, которое подозревается в деятельности иностранного агента, но не зарегистрировано в данном статусе. Основными структурами, которые осуществляют сбор данных о лице – Министерство юстиции РФ, Федеральная служба безопасности РФ, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Дела об иноагентах рассматривает также «Лига безопасного интернета» – российская околоправительственная организация, осуществляющая проведение цензуры в сети Интернет, созданная в 2011 году. Основным направлением данной организации является самоцензура (умышленное устранение автором (лицом, опубликовавшим данные материалы) из своей публикации в социальной сети или иного источника материалов, которые недопустимы или противозаконны для публичной демонстрации).

Следующим этапом процедуры является оценка деятельности «подозреваемого» лица (данная оценка проходит на основе полученных и проанализированных ранее сведений). Целью данного действия является выявление связей с иностранным государством или организацией.

Сбор таких данных проводится на основе анализа открытых источников информации. Государственные органы и специализированные службы активно изучают доступные данные, включая публикации в сети Интернет, в средствах массовой информации, социальных сетях и иных источниках информации. Исследуются все социальные сети, в том числе и отнесенные к списку запрещенных в Российской Федерации, такие как Insagram⁷, Facebook⁸ (стоит подчеркнуть, что эти социальные сети в 2022 г. признаны судом экстремистскими, поскольку Тверской суд г. Москва отметил, что «под видом коммерческой деятельности компания распространяет призывы к насилию в отношении граждан, нарушает их права и несет угрозу конституционному строю» [7]). Изучают опубликованные лицами посты, иную информацию, размещенную в социальных сетях, а также другие высказывания в формате интервью и так далее. Выявляются случаи опубликования так называемой фэйковой информации [8. С. 153; 9. С. 37]. Особому вниманию подвергаются сведения о коммерческих организациях иностранных государств, дипломатических миссиях, некоммерческих организациях.

Для более точного выявления связей с иностранными государствами, специализированными органами используются средства технического наблюдения и контроля, что включает в себя средства наблюдения, перехвата сообщений и обработки данных. При этом стоит отметить, что при данном действии специализированными органами соблюдаются все законодательные нормы и правила, гарантирующие защиту прав граждан и конфиденциальность информации (в соответствии с Федеральным законом № 152-ФЗ от 27.07.2006 [10]).

Не во всех случаях анализ открытых источников информации дает полную картину связей гражданина с иностранными государствами или организациями. Именно поэтому в таких случаях применяются разного рода оперативно-разыскные мероприятия, которые включают:

1. Обыск (вид следственного действия, которое состоит из обследования помещения либо лица (личный обыск), целью которого является обнаружение предметов или иных документов, которые имеют какое-либо значение для дела. В данном понятии такой вид применяется для обнаружения документов, подтверждающих связь с иностранными государствами и организациями [11. С. 285].

2. Следственные действия (обеспеченные силой государственного действия лиц, имеющих установленные полномочия, которые направлены на сбор и проверку доказательств по делу). В данном понятии такой вид применяется для

⁷ Социальная сеть Instagram компании Meta признана экстремистской и запрещена в РФ.

⁸ Социальная сеть Facebook компании Meta признана экстремистской и запрещена в РФ.

сбора необходимых данных о физическом лице или иной организации, подозреваемой в осуществлении деятельности иностранного агента [12. С. 223].

Дальнейшим этапом является выявление связи с иностранным государством или иностранной организацией. После завершения данного этапа компетентными органами принимается решение о возможном признании лица иностранным агентом. Такое решение основывается на общественной значимости деятельности лица.

В случае признания факта связи лица с иностранными организациями или иностранным государством, лицо обязано пройти регистрацию для осуществления официальной деятельности в статусе иностранного агента, для этого лицу или организации необходимо предоставить информацию (например, выписку из учредительных или иных документов; свидетельство о государственной регистрации и др.)

Процесс признания лица иностранным агентом может иметь серьезные последствия. В зависимости от конкретных обстоятельств, такое признание может привести к ограничению его прав и свобод, которое может включать ограничение свободы передвижения внутри страны, наложение финансовых ограничений. Кроме данных последствий, за нарушение законодательства об иностранных агентах может повлечь за собой в установленном порядке административную, уголовную и иную ответственность.

Процесс признания лиц иностранными лицами в Российской Федерации имеет цель – обеспечение прозрачности и контроля над деятельностью организаций и физических лиц, которые получают финансирование или иные ресурсы от иностранных источников, что в свою очередь, является важным механизмом обеспечения национальной безопасности и суверенитета государства.

Заключение. В настоящее время все чаще встречается в практике действие лиц, работающих в интересах иностранных государств на территории России [13]. В соответствии с действующим законодательством иностранным агентом признается лицо, которое получило или получает поддержку от иностранных организаций, а также находится под иностранным влиянием и осуществляет определенные, установленные данным законом виды деятельности. Условиями признания лица иноагентом являются: наличие иностранного финансирования, участие в политической деятельности, наличие некоммерческой организации иностранного агента.

Признание и установление статуса иноагента имеет важное значение для государства, так как таким образом открываются возможности для принятия эффективных мер по предотвращению, пресечению и нейтрализации действий, которые угрожают интересам и безопасности государства.

Список литературы

1. Корня А., Вертенникова К. Минюст пересчитал иноагентов [Электронный ресурс]. URL: <https://www.kommersant.ru/doc/5987148> (дата обращения: 05.09.2024).
2. В Минюсте назвали число действующих в России иностранных агентов [Электронный ресурс]. URL:

<https://www.gazeta.ru/politics/news/2024/02/08/22293733.shtml> (дата обращения: 05.09.2024).

3. О контроле за деятельностью лиц, находящихся под иностранным влиянием: Федеральный закон от 14.07.2022 № 255-ФЗ (ред. от 24.07.2023) // Собрание законодательства РФ. 2022. № 29 (ч. II), ст. 5222.

4. О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента: Федеральный закон от 20.07.2012 № 121-ФЗ (ред. от 04.06.2014) // Собрание законодательства РФ. 2012. № 30. Ст. 4172.

5. О некоммерческих организациях: Федеральный закон от 12.01.1996 № 7-ФЗ (ред. от 31.07.2023) // Собрание законодательства РФ. 1996. № 3, ст. 145.

6. Латыпова Э. Ю., Рогова К. М. О правовых последствиях признания лиц иностранным агентом // Семья и традиционные семейные ценности как духовно-нравственная основа развития общества и государства: сб. материалов Междунар. науч.-практ. конф. Чебоксары, 18-20 апреля 2024 г. / Чуваш. гос. ун-т им. Н. И. Ульянова. – Чебоксары: Изд-во Чуваш. гос. ун-та, 2024. С. 612–618.

7. Егоров И. Суд признал Meta экстремистской организацией и запретил в России Facebook⁹ и Insagram¹⁰ [Электронный ресурс]. URL: <https://rg.ru/2022/03/21/reg-cfo/sud-zapretil-v-rossii-instagram-i-facebook-za-ekstremistskuu-deiatelnost.html> (дата обращения: 05.09.2024).

8. Латыпова Э. Ю., Гильманов Р. Э., Воронцов И. А. О классификации видов фейковой информации применительно к уголовной ответственности за публичное распространение заведомо ложной информации // Актуальные проблемы правового, экономического и социально-психологического знания: теория и практика: материалы VI Международной научно-практической конференции. – Донецк, 2022. – С. 152–154.

9. Латыпова Э. Ю., Гильманов Р. Э. Уголовно-правовая ответственность за распространение фейков в социальных сетях // Цифровые технологии и право. Сборник научных трудов I Международной научно-практической конференции. В 6 т. / под ред. И. Р. Бегишева [и др.]. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. – С. 36–39.

10. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» // Собрание законодательства РФ. 2006. № 31 (1 ч.), ст. 3451.

11. Гриненко А. В. Уголовный процесс: учебник и практикум для среднего профессионального образования. – 9-е изд., перераб. и доп. – М.: Юрайт, 2023. 361 с.

12. Манова Н. С. Уголовный процесс: учебное пособие для вузов / Н. С. Манова, Ю. В. Францифоров, Н. О. Овчинникова. – 15-е изд., перераб. И доп. – Москва: Юрайт, 2023. – 276 с.

⁹ Социальная сеть Instagram компании Meta признана экстремистской и запрещена в РФ.

¹⁰ Социальная сеть Facebook компании Meta признана экстремистской и запрещена в РФ.

13. Траоре Д. От теории африканского происхождения человечества к современным социальным, правовым и технологическим новациям: краткий аналитический экскурс в антропосоциогенез // *Journal of Digital Technologies and Law*. – 2024. – Т. 2, № 2(2). – С. 473–486. DOI: <https://doi.org/10.21202/jdtl.2024.24>. EDN: fhsfeo

Д. В. Лобач,
кандидат юридических наук,
Университет прокуратуры Российской Федерации,
Дальневосточный юридический институт (филиал)

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПУБЛИЧНЫЕ ПРИЗЫВЫ К АГРЕССИВНОЙ ВОЙНЕ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОСТОЯНИЯ: ПЕРСПЕКТИВА МОДЕРНИЗАЦИИ

Аннотация. В статье изучаются некоторые аспекты, снижающие эффективность уголовно-правового регулирования отношений, составляющих международный мир, в современных условиях информационного противостояния. Доказывается, что публичные призывы к развязыванию агрессивной войны следует рассматривать только как часть более общего понятия пропаганды агрессии. Аргументирована позиция, в соответствии с которой общественная опасность пропаганды агрессии, осуществляемой в информационном пространстве, может быть выше по сравнению с публичными призывами к этому преступлению. Делается вывод о необходимости модернизации правовых норм об агрессии в целях повышения эффективности уголовно-правового механизма обеспечения международного мира, но с учетом положений международного права, доминант правовой политики, правил юридической техники, требований теории криминализации и общих принципов правотворчества.

Ключевые слова: уголовная ответственность за развязывание агрессивной войны, агрессия, пропаганда агрессии, информационное пространство, кибероружие

CRIMINAL LIABILITY FOR PUBLIC CALLS TO AGGRESSIVE WAR IN THE CONDITIONS OF INFORMATION CONFRONTATION: MODERNIZATION PROSPECTS

Abstract. The article examines some aspects that reduce the effectiveness of criminal-legal regulation of relations that make up international peace in the modern conditions of information confrontation. It is proved that public calls to unleash an aggressive war should be considered only as part of a more general concept of propaganda of aggression. The position is substantiated, according to which the public danger of propaganda of aggression carried out in the information space may be higher in comparison with public calls for this crime. A conclusion is made about the need to modernize the legal norms on aggression in order to increase the effectiveness of the criminal-legal mechanism for ensuring international peace, but taking into account the provisions of international law, the dominants of legal policy, the rules

of legal technique, the requirements of the theory of criminalization and the general principles of lawmaking.

Keywords: criminal liability for unleashing an aggressive war, aggression, propaganda of aggression, information space, cyber weapons

Введение. В истории международного права и практике международных отношений агрессия рассматривается как главное преступление, посягающее на международный мир, подрывающее архитектуру международной безопасности, осложняющее межгосударственные отношения, а также создающее негативные эффекты для экологической, гуманитарной, экономической и демографической безопасности. Войны ведут к деградации международного правового порядка, основанного на принципах мирного сосуществования государств и народов, уважения личных и коллективных прав, включая право на самоопределение, конструктивного участия в международном общении, добровольного выполнения международных обязательств, взаимного уважения национальных интересов. Высокая общественная опасность агрессивной войны объясняется еще и тем фактом, что возникающий вооруженный конфликт сам по себе становится криминогенным условием для совершения военных преступлений, геноцида и преступлений против человечности, а также способствует распространению терроризма, экстремизма, незаконного оборота наркотиков и оружия. Кроме того, как это хорошо доказывает история, возникновение вооруженного конфликта само по себе может стать причиной цепной реакции для последующих конфликтов, куда будут втянуты другие государства, национальные интересы которых были попорчены в результате нарушения сложившейся системы безопасности.

Основная часть. Кульминационным моментом признания общественной опасности агрессии, повлекшее дальнейшую ее криминализацию, стало окончание Второй мировой войны, унесшей десятки миллионов человеческих жизней и причинившей огромный социально-культурный вред и экономический ущерб многим государствам. Именно на Нюрнбергском военном трибунале над главными военными преступниками Второй мировой войны впервые в истории человечества была установлена уголовная юрисдикция в отношении преступлений против мира. Так, еще в 1947 г. была принята резолюция Генеральной Ассамблеи ООН «Меры, которые должны быть приняты против пропаганды и поджигателей новой войны», а в 1966 г. договорно-правовой запрет был установлен в результате принятия Международного пакта о гражданских и политических правах.

Историческая обусловленность установления уголовно-правового запрета в отношении вербальных действий, направленных на развязывание агрессивной войны, продиктована международным пониманием опасности создания в обществе социально-психологической атмосферы, способствующей всеобщему одобрению будущей войны как политически необходимого и морально оправданного решения, которое должно в конечном счете принять уполномоченный государственный орган или должностное лицо, под воздействием возникших в обществе социальных требований, ожиданий или притязаний. Другими словами, в отличие, например, от публичных призывов к осуществлению террористической деятельности, опасность которых заключается в возникновении у людей психологи-

ческой готовности совершать преступления террористического характера, публичные призывы к развязыванию агрессивной войны не могут привести к совершению этого преступления со стороны населения, так как подобного рода решения уполномочены принимать только государственные должностные лица или органы государственной власти. Однако это преступление может запустить процесс легитимизации будущей агрессии, что ускорит принятие такого решения соответствующим органом власти или должностным лицом. Такой процесс может выражаться в проведении публичных мероприятий, общественных слушаний и обсуждений в поддержку войны, широком медийном освещении острых социальных вопросов в сфере внешней политики.

Уголовная ответственность за пропаганду войны была установлена в Советском Союзе еще 1958 г. Правовая норма ст. 8 Закона СССР от 25.12.1958 «Об уголовной ответственности за государственные преступления» криминализовала пропаганду войны, в какой бы форме она не велась, закрепив наказание в виде лишения свободы на срок от трех до восьми лет и со ссылкой на срок от двух до пяти лет или без ссылки. Российская Федерация, учитывая изменившиеся геополитические реалии и признав международный мир в качестве самостоятельного объекта политико-правовой охраны в фокусе внешней политики, криминализовала как саму агрессию (ст. 353 УК РФ), так и публичные призывы к развязыванию агрессивной войны (ст. 354 УК РФ).

Обязательным условием совершения данного преступления является публичный характер призыва к развязыванию агрессивной войны. Понятие «публичные призывы» раскрывается в постановлении Пленума Верховного Суда РФ от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности». В п. 4 данного документа закреплено, что под публичными призывами следует понимать выраженные обращения к другим лицам с целью побудить их к осуществлению преступления.

Вместе с тем в условиях геополитического и информационно-технологического противостояния считаем уголовно-правовую норму ст. 354 УК РФ несовершенной по ряду причин.

Во-первых, в УК РФ отсутствует легальное определение агрессивной войны. Норма ст. 353 УК РФ в усеченном выражении текстуально повторяет нюрнбергскую модель, где агрессивная война воспринималась как политика нацистской Германии, выражаемая в применении своих вооруженных сил против других государств. Отсутствие такого определения размывает юридические границы правомерного (допустимого) и противоправного (запрещенного), а также создает сложности для квалификации, например, таких действий, как публичные призывы к началу освободительной войны, проведению гуманитарной интервенции, борьбе с транснациональным терроризмом на территории другого государства, защите своих граждан за рубежом, участию в миротворческой операции.

Как известно, впервые рабочее понятие агрессии было дано в резолюции Генеральной Ассамблеи ООН от 1974 г. «Определение агрессии». В документе закреплено общее понятие агрессии (ст. 1) и определен перечень наиболее типичных актов агрессии (ст. 3). При этом в ст. 4 этой резолюции закреплено, что Совет Безопасности ООН согласно положениям Устава ООН может признать и другие акты в качестве агрессии. Несмотря на отсылку к данному документу,

которая делается в комментариях к УК РФ, учебной и научной литературе, для уяснения правового смысла уголовно-правовых норм ст. 353 и 354 УК РФ необходимо в то же время понимать юридическую ограниченность самого документа, который является информационно-разъяснительным документом для Совета Безопасности ООН. Кроме того, недопустима ссылка на идентичное определение агрессии, отраженное в Римском статуте Международного уголовного суда, так как Россия не признает его юрисдикцию, и сам документ не порождает международных обязательств по криминализации агрессии.

Во-вторых, эскалация геополитического конфликта в эпоху Четвертой промышленной революции, характеризующейся созданием социально ориентированных информационных систем, управляющих различными сферами общественной жизни, и появлением новых технологий.

В научной среде неоднократно высказывались обоснования и делались предложения о возможности использования информационных технологий не только в целях манипулирования общественным сознанием, но и для совершения кибератак против государства в политических целях [5; 6; 9]. Например, в Военной доктрине Российской Федерации от 2014 г. (далее – Военная доктрина) неоднократно закрепляются информационные технологии в контексте фактора, лежащего в основе современных вооруженных конфликтов. Кроме того, в определении рассматриваемой военной опасности отражено особое содержание – направленность на такие объекты, как суверенитет, политическая независимость и территориальная целостность государства.

Не будет преувеличением отметить тот факт, что в условиях информационного развития социальных отношений понятие войны, ставшее классическим (было предложено в XIX в. известным военным теоретиком Карлом Клаузевицем), претерпело существенное изменение, обусловленное расширением сферы военного противостояния. В современных реалиях социальная коммуникация, взятая во всем своем многообразии, интенсивно проявляется в информационном пространстве, а само общество в силу качественных преобразований социальных связей и отношений преобразуется в социально-информационную систему, функционирующую по своим правилам и протоколам в фокусе определенных ожиданий, потребностей и интересов. Вооруженный конфликт более не сводится исключительно только к применению вооруженных сил в физической реальности, так как она трансформируется по причине широкой, массовой и интенсивной интеграции результатов научно-технического прогресса в XXI в. и социально-информационной конвергенции, при которой социальный мир все больше погружается в информационное пространство, которое в свою очередь становится сложной, многоуровневой и многофункциональной площадкой для реализации социальных отношений.

В-третьих, пропаганда агрессии является более широким понятием, охватывающим не только сами призывы, но и действия завуалированного характера, позволяющие развивать и поддерживать в обществе нетерпимое отношение к другим государствам и народам. Государственная пропаганда агрессии, направленная на объяснение и оправдание будущего применения своих вооруженных сил в целях защиты и обеспечения национальных интересов, создает условия легитимизации агрессии, а в условиях развития информационных отно-

шений становится эффективным инструментом трансформации коллективного восприятия внешних угроз.

Концепт «пропаганда» в теории информационно-психологического воздействия рассматривается в качестве функционального инструмента целенаправленного и систематического воздействия на индивидуальное и групповое сознание в целях изменения системы духовных ценностей, представлений, идей и взглядов, предопределяющего реконструкцию социальной действительности с учетом новых потребностей и ожиданий, которые соответствуют требованиям организатора пропаганды [12].

Помимо публичных призывов пропаганда также охватывает широкий диапазон различных средств, позволяющих создавать и распространять манипулятивную информацию. Внешние формы пропаганды включают литературные произведения, демонстрирующие образ врага в отношении другого государства; научные труды, доказывающие преступный характер политического режима в другом государстве и прямо или косвенно обосновывающие необходимость принятия силовых мер в целях его свержения.

Указанные формы проявления пропаганды направлены на создание образа врага, а как следствие – в стране создаются социально-психологические условия, которые в своей совокупности позволяют объяснить, оправдать и поддержать будущую инициативу применения вооруженных сил против другого государства. В контексте сказанного нельзя не отметить активную практику использования инструментов манипуляции общественным сознанием в условиях поддерживаемой государством пропаганды против других государств, иностранных органов и отдельных должностных лиц.

Такое воздействие ведет к адаптивным психологическим и социально-культурным изменениям личности, которая либо принимает новую информацию как объективную данность, либо отказывается ее признавать в качестве достоверной, попадая тем самым в психологический диссонанс, выражаемый невозможности определиться с достоверностью поступающей информации при ее многообразии. В соответствии со ставшим классическим постулатом диалектического материализма, заключаемого в том, что бытие определяет сознание, закономерно сделать допущение об относительном переходе физического социального бытия в сферу информационного пространства, в котором происходит формирование новой социально-психологической модели человека, основанной на спекулятивных нарративах. Такие нарративы создаются и развиваются в целях дискредитации других политических сил и делегитимизации государственных режимов через формирование у населения определенного негативного образа видения конкретных исторических событий. В процессе пропагандистского воздействия в информационном пространстве спекулятивный нарратив формируется фрагментарно, но в целом он представляет собой законченный событийный сюжет. При этом такой нарратив создает условия для формирования в обществе новых потребностей и ожиданий, которые предопределяют новый вектор государственной политики. Сказанное можно продемонстрировать на примере информационной агрессии против Российской Федерации, развязанной в информационном пространстве с 2008 г. Активное развитие и продвижение различных социальных сетей, мессенджеров и видеохостингов, выступающих эффективным

инструментом для продвижения брендов, привлечения аудитории и монетизации творчества, демонстрируют следующие негативные образы России: 1) Россия как исторический аутсайдер с несостоявшимся аппаратом управления; 2) Россия как угроза цивилизованному миру и демократическим ценностям; 3) Россия как государство-агрессор; 4) Россия как бескультурная страна.

Образ России как государства-агрессора основывается на распространении идей о постоянном расширении своей территории и захвате новых земель, участии в вооруженных конфликтах, милитаризации общества и агрессивной внешней политике. Например, хорошо известно, как в медийном пространстве клеймили Российскую Федерацию за участие в вооруженном конфликте с Грузией в 2008 г. Были проигнорированы предшествующие вооруженному конфликту события, а Россия представлена как государство, развязавшее войну с Грузией. При этом изначально в медийном пространстве ничего не говорилось о нападении грузинской армии на миротворческий контингент и местное гражданское население.

Отметим, что подобного рода деструктивная пропаганда, позволяющая охватить широкую аудиторию, оказывает тлетворное влияние как на население, так и на политические силы, поскольку формируются особые ожидания, выступающие триггером для принятия соответствующих мер против национальных интересов другого государства. Не будет преувеличением также сказать, что пропагандистский эффект в части склонения населения к признанию необходимости применения национальных вооруженных сил против другого государства является более действенным в сравнении с тривиальным призывом к агрессивной войне, поскольку в последнем случае склонение к вооруженному конфликту осуществляется открыто, а при пропагандистском воздействии оно носит завуалированный характер. В этом отношении пропаганда агрессии обладает более высокой степенью общественной опасности, нежели публичные призывы.

Признание пропаганды к совершению противоправных действий в качестве социальной деструкции, создающей условия для девиантного поведения, актуализирует вопрос о возможности или необходимости криминализации пропаганды агрессии. В науке уголовного права многие исследователи едины в признании общественной опасности в качестве главного основания для установления уголовно-правового запрета [1. С. 37–42; 2. С. 7–10]. Соглашаясь с этим, в то же время необходимо признать, что само явление должно быть идентифицируемым в своем онтологическом проявлении, то есть восприниматься в строго определенных параметрах индивидуального восприятия в рамках общего признания. Возможность идентификации самого явления, предопределяющего возможность раскрытия общественной опасности как особого его свойства, позволяет конституировать формально-юридические признаки данного явления в правовой норме. В противном случае налицо ситуация, когда усматриваются отдельные контуры явления или же вовсе оно воспринимается интуитивно и, как следствие, поверхностно описывается, то есть ему придается субъективная дескриптивная форма. В этом отношении пропаганда является более сложным в формально-юридическом плане социальным явлением, нежели публичные призывы, понимание которых как уже было показано выше, сложилось в судебной практике. Криминализация пропаганды агрессии без определения достаточных

для правоприменения признаков данного явления социальной действительности может привести к снижению эффективности уголовно-правового регулирования отношений, связанных с обеспечением международного мира, что может выражаться в ошибочной квалификации действий в качестве пропаганды агрессии в силу правовой неопределенности диспозитивной части правовой нормы или по причине спекулятивного применения этой нормы при необоснованной широте дискреционных полномочий.

Учитывая распространение инфоресурсов в сети «Интернет», не обладающих статусом СМИ, а равно массовое использование таких ресурсов, следует сделать логическое допущение о не меньшей степени общественной опасности информационно-телекоммуникационных сетей в сравнении со СМИ. Массовое использование населением информационных ресурсов в сети «Интернет» существенно повышает вероятность стать объектом деструктивного воздействия со стороны лиц, которые совершают вербальные преступления, включая призывы к агрессивной войне.

Заключение. Необходимо отметить, что криминализация публичных призывов к развязыванию агрессивной войны основывается как на признании общественной опасности самой агрессии, выступающей главной угрозой для мирного сосуществования государств и народов, так и на международной политике, направленной на предупреждение актов агрессии через запрещение публичных призывов к противоправному применению своих национальных вооруженных сил против суверенитета, политической независимости и территориальной целостности другого государства. Однако, учитывая изменение природы (политической, организационной, телеологической, социально-психологической сущности) вооруженного конфликта, происходящей во многом под воздействием факторов глобализации, развития научно-технического прогресса, качественного изменения социальных связей, включая цифровую информатизацию социальных отношений, представляется необходимым модернизация правовых норм об агрессии в целях повышения эффективности уголовно-правового механизма обеспечения международного мира, но с учетом положений международного права, доминант правовой политики, правил юридической техники, требований теории криминализации и общих принципов правотворчества. Положения международного права необходимо учитывать в части заимствования уже сложившегося в практике международных отношений определения агрессии, но с обязательным восприятием общих принципов международного права. Доминанты правовой политики отражают конкретные ориентиры внешней политики, которые закреплены в стратегических документах. Особое внимание необходимо обратить на положения теории криминализации, которые, к сожалению, часто игнорируются законодателем или вольно интерпретируются в научной сфере.

Список литературы

1. Иванов Н. Г. Общественная опасность деяния как онтологическая основа криминализации: монография. – Москва: Проспект, 2016. – 80 с.
2. Ищенко И. В. Общественная опасность как интегративное свойство. М.: Проспект, 2023. – 162 с.

3. Каропова С. Г., Некрасов С. В., Пинчук А. Н. Пропаганда как метод воздействия на общественное сознание: общий теоретический аспект // Вестник НГУЭУ. – 2020. – № 4. – С. 212–229.

4. Конышев В. Н., Парфенов Р. В. Гибридные войны: между мифом и реальностью // Мировая экономика и международные отношения. – 2019. – Т. 63, № 12. – С. 56–66.

5. Карасев П. А. Эволюция национальных подходов к ведению кибервойны // Международная аналитика. – 2022. – № 13 (2). – С. 79–94.

6. Лобач Д. В., Смирнова Е. А. Компьютерные сетевые атаки как акт агрессии в условиях развития современных международных отношений: pro et contra // Российский журнал правовых исследований. – 2020. – Т. 7, № 4. – С. 59–65.

7. Порецкова А. А. Концептуализация теоретических подходов к изучению политической пропаганды // Контуры глобальных трансформаций: политика, экономика, право. – 2015. – Т. 8, № 2 (40). – С. 19–33.

8. Саяпин С. В. Определение преступления агрессии и национальные уголовно-правовые системы // Международное правосудие. – 2012. – № 1 (2). – С. 87–97.

9. Тимошков С. Г. Кибератака как современная форма совершения акта агрессии // Вестник РГГУ. Серия «Экономика. Управление. Право». – 2017. – № 1 (7). – С. 127–135.

10. Gianpiero G. Cyber-Attacks as Aggression Crimes in Cyberspace in the Context of International Criminal Law // European Journal of Social Sciences Studies. – 2020. – Vol. 4, Iss. 1. – Pp. 40–46.

11. Värk R. The Legal Framework of the Use of Armed Force Revisited // Baltic Security & Defence Review. – 2013. – Vol. 15, Iss. 1. – Pp. 56–94.

12. Woolley S.C., Howard Ph. N. Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. – New York: Oxford University Press, 2019. Pp. 3–20. – 263 p.

Т. М. Лопатина,

доктор юридических наук, профессор,
Смоленский государственный университет

НАУЧНО-ТЕХНИЧЕСКИЙ ПРОГРЕСС КАК ФАКТОР ТРАНСФОРМАЦИИ УГОЛОВНОГО ПРАВА

Аннотация. В статье рассматривается влияние процесса цифровизации общества на правовую сферу, в частности на уголовное право и уголовное судопроизводство. Обоснована точка зрения о том, что развитие технологии искусственного интеллекта приведет к трансформации экономики, общества, что потребует, в свою очередь, модификации права и пересмотра существующей уголовно-правовой системы. Предметом изучения выступили возможные риски в сфере уголовно-правового регулирования в условиях нарастающего доминирования цифровых технологий, недостаточно исследованные в отечественной науке уголовного права.

Ключевые слова: искусственный интеллект, правовое регулирование, квалификация преступлений, цифровое судопроизводство, компьютерные преступления, цифровые технологии

SCIENTIFIC AND TECHNOLOGICAL PROGRESS AS A FACTOR IN THE TRANSFORMATION OF CRIMINAL

Abstract. The article examines the impact of the process of digitalization of society on the legal sphere, in particular, on criminal law and criminal proceedings. The author substantiates the point of view that the development of artificial intelligence technology will lead to the transformation of the economy and society, which in turn will require modification of law and revision of the existing criminal legal system. The subject of the study was the possible risks in the field of criminal law regulation in the context of the increasing dominance of digital technologies, insufficiently investigated in the domestic science of criminal law.

Keywords: digital technologies, legal regulation, artificial intelligence, qualification of crimes, digital legal proceedings, computer crimes

Введение. Движителем развития цивилизации является научно-технический прогресс, который формирует новые экономические реалии и влечет соответствующие изменения в правовом регулировании. Так, первая промышленная революция XIX века (1760–1840-е годы) инициировала переход к механическому производству, что привело к созданию новых средств транспортировки грузов и расширению рынков сбыта. Научно-технические достижения на фоне буржуазных революций выступили катализатором качественных изменений в праве и его формирование в привычных для нас формах. Например, формирование института частной собственности (Гражданский Кодекс Наполеона) и его уголовно-правовая охрана под угрозой смертной казни, пожизненных или срочных каторжных работ (ст. 381, 382, 385, 400 Уголовного Кодекса Франции 1810 г.) [7].

Вторая промышленная революция (70-е годы XIX века – 60-е годы XX века) характеризуется промышленным бумом, обеспеченным электрификацией и конвейерным производством, урбанизацией населения и значительными правовыми новациями, изменившими структуру всей системы права. Появились новые отрасли права, расширился перечень объектов уголовно-правовой охраны.

Третья революция, так называемая информационная, произошла в середине 20-го века под эгидой Соединенных Штатов и отмечена массовой автоматизацией, компьютеризацией и роботизацией производства. В уголовные кодексы вводятся нормы, предусматривающие ответственность за преступления в сфере компьютерной информации, противоправные действия в отношении программного продукта криминализируются.

В настоящее время дискутируется вопрос о начале периода четвертой промышленной революции, опирающейся на использование искусственного интеллекта и производство продукции обучающимися машинами.

Основная часть. Четвертая промышленная революция подразумевает интеграцию искусственного интеллекта, квантовых вычислений, автономных роботизированных процессов в повседневную жизнь человека и общества. Все это

неизбежно ведет к ускорению технического прогресса и движению к некой точке: технологической сингулярности, после чего люди превратятся в киборгов, или киборги будут вести себя как люди. Широкое государственно-частное применение цифровых технологий кардинально меняет среду пребывания, формируя новые формы взаимодействия между субъектами общественных отношений. В обозначенных условиях глобальной цифровизации имеет место нарастающая проблема адекватного правового регулирования системы управления цифровыми социально-правовыми отношениями.

В рамках формирующейся новой среды традиционные инструменты правового регулирования становятся не эффективными. Требуется переосмысления сущности права. Инновации должны получить соответствующее законодательное оформление в уголовном праве и уголовном процессе. Например, Великобритания уже внедрила виртуальные судебные процессы, в которых все участники взаимодействуют через выделенную защищенную сеть. Саудовская Аравия перешла на электронное ведение уголовных дел. Соединенные Штаты разработали Электронный уголовный кодекс. Между тем Российское традиционное материальное право продолжает существовать в аналоговом режиме, медленно реагируя на стремительное движение общества к цифровому формату.

Появление нового вида преступлений с использованием информационно-телекоммуникационных технологий увеличило общественную опасность всей преступности и степень криминогенности глобальной сети Интернет. Констатируется двоякая ситуация, при которой, с одной стороны, имеет место процесс «цифровизации» преступности, к примеру наркопреступности, с другой – потенциал уголовного закона по противодействию преступности оказывается недостаточным, например, в части обеспечения наркобезопасности общества. В связи с этим следует разделить позицию С.Я. Лебедева о «явной неготовности нашего законодателя и, главное, правоприменителя адекватно реагировать на происходящие в мире технологические перемены» [2. С. 17–25]. Очевидна необходимость в условиях развития технологий искусственного интеллекта объединения профессиональных потенциалов экономистов, юристов и IT-специалистов с целью создания условий для трансформации права и решения проблемы обеспечения безопасности личности, общества и государства. В противном случае существует угроза кризиса правоприменения.

Повышенная общественная опасность цифровой преступности обусловливается доступностью информационных технологий для рядового пользователя, увеличение количества граждан, имеющих навыки работы с компьютером. «Динамика прироста преступлений в сфере компьютерной информации с 2017 по 2019 годы составила 165 %» [3]. За 2023 год прирост преступлений с использованием информационно-телекоммуникационных технологий составил +29,7 % (67 6951), а их удельный вес возрос до +25,8 %. К примеру, рост только компьютерных мошенничеств в сравнении с 2022 годом составил +38,2 % (35 6079). «По данным Генеральной Прокуратуры РФ число IT-вымогательств в 2023 году выросло на 10 % в сравнении с 2022 годом и достигло 79 %» [3]. Данный вид преступлений характеризуется возможностью совокупности с иными преступлениями, например, преступлениями террористического характера или экстремистской направленности.

Наиболее распространенными являются следующие способы совершения цифровых преступлений:

- использование социальных сетей (через несанкционированный доступ к персональным аккаунтам пользователя сети Интернет). Преступник просит номер мобильного телефона жертвы, со счета которого похищаются деньги, либо он используется как промежуточное звено для перевода чужих денежных средств в мошеннической цепи, чтобы запутать следы.

- Звонок от псевдо-представителя банка, когда преступник от имени сотрудника банка сообщает о подозрительных действиях по карте гражданина (например, кто-то пытается оформить кредит). Получив необходимую информацию о реквизитах карты, преступник похищает денежные средства с банковского счета.

- Предоплата, когда преступник, выступая в роли покупателя, находит продавца на интернет-площадке и в процессе переписки сообщает, что готов совершить покупку и уже отправил предоплату. Для получения денежных средств жертва мошенника переходит по ссылке на поддельную страницу официального сайта банка. Получив таким образом доступ к конфиденциальным сведениям продавца, преступник совершает хищение.

- Использование приложений «Авито», когда преступник размещает объявление на интернет-площадке о продаже товара по низкой цене. Во время общения с покупателем преступник предлагает оформить доставку. Для оплаты услуги покупателю высылается ссылка на поддельную страницу торговой площадки, где просят ввести данные его платежной карты, потом применяется обычная схема обмана покупателя.

Приведенный перечень не является исчерпывающим, поскольку способы совершения цифровых преступлений транслируют определенное противоречие между их комбинаторностью и устойчивой повторяемостью. По мнению В. Н. Карагодина, «типизация подобных методов будет повышаться по мере разработки экспертных программ, предназначенных для оценки и корректировки уже реализуемых программных средств» [1. С. 19].

При нарушении общественных отношений с применением цифровых технологий уголовно-правовое регулирование охватывает следующие сферы, а именно:

- криминализация деяний, в которых цифровые технологии выступают способом преступной деятельности. Уголовное законодательство не успевает своевременно реагировать ввиду разнообразия и вариантности преступной деятельности. Например, публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет (ч. 2 ст. 205² УК РФ) были криминализированы Федеральным законом № 153-ФЗ в 2006 году, а мошенничество в сфере компьютерной информации (ст. 159⁶ УК РФ) – Федеральным законом № 207-ФЗ в 2012 году;

- проблематика современного уголовного права должна быть ориентирована на решение вопроса об уголовной ответственности органоидного искусственного интеллекта в качестве субъекта права.

Заключение. Таким образом, стержневой составляющей новой производственной революции, без сомнения, являются информационные технологии. Применительно к сфере уголовно-правовых отношений актуализируются следующие ключевые составляющие.

Во-первых, цифровая форма уголовного судопроизводства и решение проблем квалификации преступлений с применением новых информационных технологий. Относительно последнего, интересным выглядит предложение о принятии Федерального закона РФ, легализующего применение судебной психологической экспертизы по выявлению признаков достоверности информации (полиграф) как одного из инструментов формирования доказательственной базы. По мнению С. А. Роганова, «с развитием науки перечень технических средств, используемых в судопроизводстве для получения доказательств в целом и при производстве отдельных процессуальных (следственных) действий в частности, пополняется. Полиграф должен быть включен в законодательный перечень технических средств, допустимых при допросе» [4. С. 45].

Противоположной позиции придерживается Верховный Суд РФ, который по кассационным жалобам осужденного Орлова Е. С. и потерпевшей П. на приговор Ленинградского областного суда от 21 мая 2021 года и апелляционное определение судебной коллегии по уголовным делам Второго апелляционного суда общей юрисдикции от 16 августа 2021 года указал, что «для психофизиологического исследования с использованием полиграфа, отсутствуют научно обоснованные методики, что не позволяет использовать полученные результаты в качестве доказательства по делу» [8].

Обозначенные кардинально разнящиеся подходы к возможной легализации полиграфа демонстрируют аналоговость уголовного судопроизводства в части возможности использования технических средств для формирования доказательственной базы и не снимают остроты проблематики применения иных технических инноваций.

Во-вторых, использование информационных технологий при принятии сначала администрацией исправительного учреждения, а затем и судом решения об условно-досрочном освобождении заключенного (например, компьютерное отслеживание динамики позитивного изменения нравственного профиля осужденного), а также информатизация процесса контроля при условно-досрочном освобождении как один из современных методов снижения рецидивной преступности.

Анализ уголовной статистики МВД России свидетельствует о сохранении на значительно высоком уровне в общеуголовной преступности доли рецидивной преступности. «Лицами, ранее совершавшими преступления, совершается до 60% новых преступлений. В структуре рецидивистов 46% занимают лица с двумя и более судимости. В течение года после освобождения из исправительного учреждения рецидив допустили 8,0 % освобожденных» [6. С. 19–22]. Одной из причин рецидива является неэффективность мер социально-правовой профилактики преступности, что обуславливает необходимость применения определенного набора технических средств для мониторинга поведения осужденных (например, электронного мониторинга), а также лиц, условно-досрочно освободившихся. Практика других государств в рассматриваемой сфере свидетельству-

ет о том, что система электронного мониторинга давно применяется к осужденным на срок не более трех лет в Австрии, а в Эстонии СЭМПЛ применяется ко всем осужденным, подлежащим условно-досрочному освобождению.

В-третьих, необходимость реагирования на цифровую эпидемиологию как новейший инструмент мониторинга, к примеру, за потреблением и распространением наркотических средств и психоактивных веществ.

Противодействие процессу адаптирования технологии искусственного интеллекта, нейросетей к применению в криминальном бизнесе, что позволит существенно расширить организованные формы преступной деятельности, требует ускорения и технической инновации. В качестве примера можно привести деятельность по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их аналогов.

Следует признать рациональное зерно в позиции В. С. Соловьева в части того, что «применение нейросетевых технологий для идентификации наркомаркетов в информационно-телекоммуникационной сети Интернет, а также анализ и систематизация информации о их деятельности положительным образом отразится на эффективности противодействия наркопреступности» [5. С. 349–360].

Таким образом, современная действительность характеризуется цифровизацией всех сторон жизни общества. Этот процесс является необратимым и его всеобщее влияние будет только нарастать как в сфере правотворчества, так и в сфере правоприменительной деятельности, обозначая для науки новые аспекты исследований. При этом, проблематика, связанная с правовыми последствиями причинения вреда искусственным интеллектом и вопросами его возмещаемости, а также создание компьютерных алгоритмов квалификации преступлений и цифровых платформ уголовного судопроизводства, остаются пока без решения. Видимо присутствует опасение, что решение, выданное с использованием технологии искусственного интеллекта, не будет отвечать принципу справедливости. Может ли компьютер учесть все жизненные обстоятельства совершения общественно опасного деяния? Эти вопросы являются дискуссионными в ближайшей научной перспективе.

Список литературы

1. Карагодин В. Н. Особенности способов преступлений, совершаемых с использованием цифровых технологий // Академическая мысль. – 2020. – № 2(11). – С. 17–20.
2. Лебедев С. Я. Цифровой безопасности – цифровой уголовно-правовой ресурс // Криминология: вчера, сегодня, завтра. – 2019. – № 4(55). – С. 17–25.
3. Никуленко А. В. Отдельные вопросы кибербезопасности в современном мире: взгляд дилетанта (возвращаясь к теме) // Право, цифровизация и безопасность в преступноведческом поле. – URL: <https://www.criminologyclub.ru/home/the-last-sessions/373-2019-12-08-11-57-27> (дата обращения: 03.07.2024).
4. Роганов С. А. Правовые основы использования полиграфа в правоохранительной деятельности Российской Федерации: учеб. пособие. – СПб.: Изд-во СПб ГЭУ, 2018. – 67 с.

5. Соловьев В. С. Криминологические риски применения технологии искусственного интеллекта в незаконном обороте наркотиков // Юридические науки. – 2021. – Т. 7(73), № 4. – С. 349–360.

6. Филиппова О. В. Структура российской рецидивной преступности // Уголовно-исполнительная система: право, экономика, управление. – 2024. – № 2. – С. 19–22.

7. Уголовный кодекс 1810 г. – URL: https://pnu.edu.ru/ru/faculties_old/full_time/isptic/iogip/study/studentsbooks/histsources2/igpzio50 (дата обращения: 02.09.2024).

8. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 28.06.2022 № 33-УД22-11-А2. – URL: <https://legalacts.ru/sud/kassatsionnoe-opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-28062022-n-33-ud22-11-a2> (дата обращения: 06.09.2024).

Ю. Ю. Малышева,
кандидат юридических наук, доцент,
Казанский институт (филиал) Всероссийского государственного
университета юстиции (РПА Минюста России)

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ ВЗЯТКИ И ПОДАРКА В ЦИФРОВОМ ПРОСТРАНСТВЕ

Аннотация. Целью исследования является разграничение взятки и подарка в уголовно-правовом аспекте данных категорий, которые сегодня беспрепятственно существуют в цифровом пространстве, а также разделение изучаемых понятий в теории и на практике, что иногда представляется крайне сложным. Сложности правоприменения заключаются в том, что нередко взятку принимают за подарок, и наоборот, поэтому мы постарались в своей научной статье дать весьма четкие критерии разграничения. Цифровое пространство современного мира дает колоссальные возможности для получения и дачи взятки, для дарения и принятия подарков, но будучи предельно схожими по форме и содержанию, взятка и подарок до сих пор не нашли должного разграничения в уголовно-правовом поле. Острота проблемы разграничения взяточничества как наиболее яркого коррупционного преступления современности с обычным принятием подарков не вызывает сомнений, поскольку с ней сталкивается каждый преподаватель, каждый доктор, государственные служащие, работники правоохранительных органов и многие другие. Установление допустимых границ и условий дарения и принятия подарков является важнейшим фактором отграничения подарка от взятки, являющимся для теории и практики уголовного права камертоном определения ясного понимания глубокого смысла данной категории.

Ключевые слова: взятка и подарок в цифровом пространстве, разграничение взятки и подарка в уголовно-правовом поле, коррупционное преступление, коррупция, цифровые технологии, подарок, взятка, цифровое пространство

CRIMINAL LEGAL ASPECTS OF BRIBE AND GIFTS IN THE DIGITAL SPACE

Abstract. The purpose of the study is to distinguish between a bribe and a gift in the criminal legal aspect of these categories, which today exist unhindered in the digital space, and also to separate the concepts being studied in theory and in practice sometimes seems extremely difficult. The difficulties of law enforcement lie in the fact that a bribe is often mistaken for a gift, and vice versa, although in our scientific article we tried to give very clear criteria for the distinction. The digital space of the modern world provides enormous opportunities for receiving and giving bribes, and for giving and accepting gifts, but being extremely similar in form and content, a bribe and a gift have not yet found proper differentiation in the criminal legal field. The severity of the problem of distinguishing bribery as the most striking corruption crime of our time from the usual acceptance of gifts is beyond doubt, since every teacher, every doctor, civil servants, law enforcement officers and many others face it. Establishing acceptable boundaries and conditions for giving and accepting gifts is the most important factor in distinguishing a gift from a bribe, which is a tuning fork for the theory and practice of criminal law in determining a clear understanding of the deep meaning of this category.

Keywords: bribe and gift in the digital space, distinction between bribe and gift in the criminal legal field, corruption crime, corruption crime, corruption, digital technology, gift, bribe, digital space

Введение. Коррупция, к сожалению, является неотъемлемым негативным явлением современной жизни, а цифровое поле выступает тем пространством, где данное социальное явление успешно процветает. Все сферы социальной, экономической, духовной и различных других сфер нашего общества оплетены паутиной коррупции, где должностное лицо злоупотребляет служебным положением в личных целях, используя свою власть и предоставленные ему права, а также влияние, возможности, льготы и контакты, связанные с его должностью, в личных целях, в нарушение законодательных и этических принципов [2. С. 23].

Когда говоришь о коррупции, первая мысль возникает о взяточничестве, которое в действительности и является самым распространенным коррупционным преступлением. Ежегодный рост коррупционных преступлений заключается в том, что в современной России очень низкий уровень правовой и этической культуры населения [1; 2. С. 173; 11].

Основная часть. Когда речь идет о даче и получении взятки, зачастую вызывает определенные сложности разграничение данного явления с дарением и приемом подарков. К большому сожалению, этическое воспитание граждан иногда не позволяет разграничить данные неоднозначные категории. Хотя считаем вполне приличным и даже весьма культурным подарить подарок доктору или преподавателю в знак благодарности за эффективное лечение, удачно проведенные роды или глубокие научные знания. Некоторые данные действия расценивают как взятку, что является неверным и некорректным представлением о данного рода категориях.

Для большинства граждан считается нормальным благодарить должностное лицо за оказание какой-либо помощи в виде передачи материальных ценностей, что свидетельствует о недостаточной осведомленности о законе, такое поведение ставит под угрозу не только социальное обеспечение, но и безопасность всей страны [4. С. 60]. Тем не менее никогда не бывает зазорным подарить преподавателю или доктору цветы по случаю дня рождения, удачно выполненной операции или в знак признательности за хорошие знания и успешный процесс завершения изучения учебной дисциплины. Никто не считает, что дарить цветы артистам не допустимо, тем не менее дарить цветы доктору или преподавателю почему-то считается взяткой, по мнению некоторых граждан. Напротив, по нашему видению, учитывая важность и нужность профессии врача и преподавателя, считаем вполне этичным и приличным приносить цветы, к примеру, на экзамен преподавателю, ни в коем случае при этом не подпадая под подкупное преступление.

Являются ли цветы взяткой? Представляется, что расценивать цветы или конфеты в качестве взятки абсурдно. Букет цветов так же, как и коробка конфет никого ни к чему не обязывает, но показывает уважение к человеку, неважно, мужчине или женщине, представителю любой должности и профессии. В соответствии с законом должность и профессия не имеют гендерной принадлежности, поскольку есть должность, к примеру, «заведующий кафедрой», «врач высшей категории», «заведующий гинекологическим отделением» и т. д.

На наш взгляд, взяточничество можно сравнить с кислотой, которая разъедает правовое поле, оставляя язвы в государственной системе, тем самым накладывая негативный отпечаток на всю сферу государственной службы, что дает людям основание полагать, что если удастся умиротворить «нужных людей», то будут независимы от законов [5. С. 97], но путать данное коррупционное преступление со взяткой в виде цветов по случаю дня рождения или сладкого новогоднего подарка по случаю праздника не верно.

За девять месяцев 2023 года в суды направлено 7 949 уголовных дел о коррупционных преступлениях в отношении 8 898 лиц. Большинство коррупционных преступлений представляют собой именно подкупные преступления, связанные со взяточничеством.

К уголовной ответственности за преступления коррупционной направленности привлечено 336 лиц, +2% по сравнению с таким же периодом прошлого года), обладающих особым правовым статусом. Среди них 174 должностных лица органов местного самоуправления, 9 депутатов законодательных органов субъектов Российской Федерации, 1 депутат Государственной Думы, 47 адвокатов, 51 член избирательных комиссий, 36 руководителей следственных подразделений и следователей правоохранительных органов, 10 прокуроров и их помощников, 6 судей.

Если сравнивать с 2020 годом, то за 9 месяцев в суды было направлено 6,3 тысяч уголовных дел коррупционной направленности, в связи с чем можно сделать вывод, что коррупционные преступления поднялись почти на 9% всего лишь за 3 года.

Кроме того, даже если речь идет о понятиях и признаках взяточничества как должностного преступления, эти категории ранее были известны российско-

му уголовному законодательству, и по-прежнему существуют значительные проблемы в понимании, толковании этих понятий и применении законодательных положений, что как раз и затрудняет разграничение данной категории с понятием и признаками подарка. Данные проблемы дополняются конфликтами между российскими законодательными ветвями власти, которые существенно усложняют борьбу со взяточничеством, а также и другими преступлениями против государственной власти, интересов государственных служб, а также эффективности борьбы с коррупцией в целом [6. С. 132]. Все это должно быть решено на научном, а в особенности на законодательном уровне уголовного права.

Совершенствование действующих норм уголовного права, а также норм других отраслей российского права и правоприменительной практики позволит добиться более высокой эффективности в борьбе со взяточничеством, другими видами коррупции и общеуголовными преступлениями. Поэтому не стоит путать взятку и подарок в виде цветов или конфет, к примеру, с выгодами материального характера и не доводить до абсурда невозможность дарения цветов или конфет преподавателю или врачу.

Рассматривая взяточничество с точки зрения юридической науки, следует отметить, что содержание этого термина раскрывается по-разному – с точки зрения узкого и широкого подходов [7. С. 144].

Сторонники «узкого» подхода отождествляют взяточничество с получением взятки или при характеристике взяточничества сводят последнее только к получению взятки, приходя к мысли, что рассматривать дачу взятки наряду с ее получением не целесообразно. Такой подход представляется в корне неверным, из-за связи между получением взятки и дачей взятки, составляющие характеристики одного из действий будут неполными, поскольку невозможно описать получение взятки абстрактным образом в полной форме, не рассматривая непосредственно дачу взятки [8. С. 195], что в цифровом поле является доступным каждому пользователю банковской карты.

Кроме того, после отнесения взяточничества к преступлениям, нарушающим порядок управления, показано, что такое поведение нарушает нормальную деятельность государственного аппарата, то есть является объектом должностных преступлений [9. С. 69]. Учитывая направление и характеристики взяточничества, представляется, что такого рода поведение является преступлением в сфере служебной деятельности и не может рассматриваться отдельно от получения взяток. Вопреки узкому толкованию понятия «взяточничество», существует его широкое толкование [10. С. 119]. Согласно этому толкованию, «взяточничество» – общее понятие, охватывающее четыре вида преступлений в уголовном законе.

Таким образом, взяточничество – собирательное понятие, охватывающее получение должностным лицом незаконной материальной выгоды (взятки) или ее предоставление за совершение должностным лицом каких-либо действий, входящих в круг его должностных обязанностей [12. С. 88], когда подарок представляет собой добровольное безусловное явление, независимое ни от каких обстоятельств (суммы подарка, времени его дарения и т. д.).

Заключение. Делая вывод по нашему исследованию, хотим сказать, что необходима конкретизация предметов взятки в законе, обязательно установление

формальных и материальных границ предмета взятки во избежание путаницы таких категорий, как «взятка» и «подарок».

Список литературы

1. Антикоррупционная этика и служебное поведение: науч.-практич. пособие / под ред. И. И. Кучерова, А. М. Цирина. М.: ИНФРА-М: 2018.
2. Гончарова О. А. Взятничество: от явления к преступлению // Эволюция российского права: материалы XVI Международной научной конференции молодых ученых и студентов, Екатеринбург, 27 апреля 2018 года / Уральский государственный юридический университет. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2018. – С. 22–25. – EDN XQEKSL.
3. Зайцев С. А. Взятничество: ретроспективный анализ регламентации преступного явления // Общество и наука: векторы развития: материалы Всероссийской научно-практической конференции, Чебоксары, 26 апреля 2023 года. – Чебоксары: Общество с ограниченной ответственностью «Центр научного сотрудничества "Интерактив плюс"», 2023. – С. 172–176. – EDN ZAMUKJ.
4. Корсаков К. В. К вопросу о разграничении понятий «подарок» и «взятка» / К. В. Корсаков, М. А. Сажая // Российская юстиция. – 2018. – № 2. – С. 60–62. – EDN YPBXJE.
5. Малышева Ю. Ю. Служебный подлог в медицинской деятельности как коррупционное преступление современности // Практика противодействия коррупции: проблемы и достижения: XII Всероссийская научно-практической конференция с международным участием, Казань, 09 декабря 2021 года. – Казань: Казанский национальный исследовательский технологический университет, 2022. – С. 95–101.
6. Малышева Ю. Ю. Антикоррупционная политика государства в сфере здравоохранения: эффект оптимизации медицины // Актуальные проблемы организации правоохранительной и правозащитной деятельности: материалы Всероссийской научно-практической конференции, Тула, 31 января 2023 года. – Тула: ВГУЮ (РПА Минюста России), 2023. – С. 130–134. – EDN SQPIXR.
7. Малышева Ю. Ю. Уголовно-правовые и криминологические аспекты служебного подлога в медицинской деятельности // Вестник Волжского университета им. В.Н. Татищева. – 2023. – Т. 1, № 2(104). – С. 142–149. – DOI 10.51965/2076-7919_2023_1_2_142. – EDN OFNFEW.
8. Малышева Ю. Ю. Взятка и подарок: уголовно-правовые и криминологические аспекты // Вестник Казанского юридического института МВД России. – 2013. – Т. 4, № 5. – С. 194–198. – EDN AVPFOM.
9. Малышева Ю. Ю. Понятие коррупционного преступления по уголовному законодательству современной России // Национальные интересы: приоритеты и безопасность. – 2012. – Т. 8, № 36(177). – С. 68–71. – EDN PCVHXL.
10. Марьина М. И. Разграничение понятий «подарок» и «взятка». К вопросу о разграничении понятий «подарок» и «взятка» // Символ науки: международный научный журнал. – 2023. – № 6-1. – С. 118–120. – EDN FPOMXS.

11. Противодействие коррупции: новые вызовы: монография / С. Б. Иванов, Т. Я. Хабриева, Ю. А. Чиханчин [и др.]; отв. ред. Т. Я. Хабриева. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М, 2018.

12. Яшков С. А. «Взятка-благодарность» или подарок: об уголовно-правовой оценке получения преподавателем вознаграждения за прием экзамена (зачета) // Вестник Академии Следственного комитета Российской Федерации. – 2016. – № 1(7). – С. 87–89. – EDN WTRLJL.

Р. Н. Малышкин,
кандидат юридических наук,
Казанский инновационный университет
имени В. Г. Тимирязева

ЭЛЕКТРОННОЕ (ЦИФРОВОЕ) УГОЛОВНОЕ ДЕЛО: НЕИЗБЕЖНАЯ РЕАЛЬНОСТЬ

Аннотация. В статье поднимаются дискуссионные вопросы о неизбежном переходе к электронной форме судебного производства на стадии предварительного расследования, представлено определение «электронное уголовное дело», приведен анализ позиций исследователей перехода к цифровому уголовному судопроизводству, на основе исследований и данных, в ходе опроса следователей Следственного комитета Российской Федерации и следователей следственных органов МВД Российской Федерации. В результате сделаны прогнозы некоторых проблем, связанных с внедрением государственной автоматизированной системы применения электронного уголовного дела.

Ключевые слова: цифровое уголовное дело, электронное уголовное дело, цифровизация уголовного процесса, VR-технологии, DDoS-атаки, цифровизация

ELECTRONIC (DIGITAL) CRIMINAL CASE: AN INESCAPABLE REALITY

Abstract. The article raises controversial issues about the inevitable transition to the electronic form of judicial proceedings at the stage of preliminary investigation, presents the definition of "electronic criminal case", provides an analysis of the positions of researchers of the transition to digital criminal proceedings, based on research and data, during a survey of investigators of the Investigative Committee of the Russian Federation and investigators of investigative bodies of the Ministry of Internal Affairs of the Russian Federation. As a result, forecasts of some problems related to the introduction of a state automated system for the application of electronic criminal proceedings have been made.

Keywords: digital criminal case, electronic criminal case, digitalization of the criminal procedure, VR technologies, DDoS attacks, digitization

Введение. Практически все сферы государственного регулирования в настоящее время прошли процедуру цифровизации. Где-то в большей степени, где-то цифровизация пока коснулась лишь краем. Сама цифровизация в нашей стране как идея «цифрового государства» стала внедряться еще с конца 90-х [1].

Так, в 1998 году Комитетом по информационной политике Государственной Думы 15 октября 1998 года была рассмотрена и принята «Концепция государственной информационной политики Российской Федерации». Чуть позднее на основе Концепции была разработана Федеральная целевая программа «ФЦП: Электронная Россия», которая в дальнейшем дала развитие различным направлениям. С этого момента, можно сказать, началось развитие эры государственного правительства и поэтапное внедрение цифровых технологий в систему государственного управления, в том числе и в области правоохранительной деятельности. Однако на первоначальном этапе программа продвигалась достаточно медленно. Причиной тому были сложности во внедрении программы, недостаточной развитости инфраструктуры. Основной проблемой был низкий уровень доступа к высокоскоростному интернету. Как только проблему удалось разрешить, внедрению цифрового управления уже серьезно ничего не мешало. Однако из-за специфичности правоохранительной деятельности внедрение таких технологий в уголовное судопроизводство пока проводилось лишь частично. Так, появились информационные базы данных, позволяющие быстро обмениваться информацией между ведомствами, оказывать услуги гражданам в кратчайшие сроки, сократилась бюрократическая нагрузка на органы власти, связанная с бумажным документооборотом. Судебная система получила свои информационные базы данных, которые решают ряд задач в совершенствовании правосудия, упрощают доступ к нему граждан, повышают общий уровень правовой культуры, решают другие задачи. Но все же уголовно-процессуальная деятельность осталась за рамками развития «цифрового государства», что, считаем, не верно.

Основная часть. В рамках изучаемого предмета необходимо определиться с некоторыми понятиями. Термин «уголовное дело» не имеет законодательного определения. Статья 5 Уголовно-процессуального кодекса Российской Федерации (УПК РФ), включающая в себя понятийный аппарат уголовного процесса не раскрывает этого понятия. Есть понятие уголовное судопроизводство, а вот понятия «уголовное дело» нет. В целом, это может и не важно, каждый судья, следователь, дознаватель понимает, что уголовное дело – это совокупность задокументированных на материальном носителе следственных и иных действий, иных материалов с применением способов фиксации, определенных законом. В научной среде уже сформировался подход, что уголовно-процессуальный акт – внешняя форма выражения принимаемых решений и на их основе действий уполномоченных на то должностных лиц. Они формируются, в том числе органами предварительного следствия [2. С. 79]. И. Н. Гимазетдинова справедливо заметила, что диспозиция части 2 статьи 474 УПК РФ вводит возможность выполнения уголовно-процессуальных актов не только типографским способом, но и электронным [3. С. 2]. Таким образом, сам УПК РФ уже предусмотрел в Разделе XIX возможность электронного документооборота. Так, ст. 474.1 УПК РФ предусматривает использование такой системы как «Единый портал государственных и муниципальных услуг (функций)» или других систем, которые используются судами и Судебным департаментом при Верховном Суде РФ, а также другие информационные системы участниками уголовного судопроизводства, использующих их при межведомственном взаимодействии. Такой порядок позволяет участникам делать запросы, подавать жалобы, ходатайства и заявления,

обращаться и получать услуги иным образом. По смыслу понимается, что заявитель получает возможность доступа к информации непосредственно на материальном носителе, либо если она оцифрована, в электронном виде. Но заметим, что законодатель заложил основу для перехода к электронному уголовному делу. самого определения, как и порядка ведения уголовного процесса, полностью в электронном (цифровом) виде пока не разработано. Есть отдельные нормы, которые пока что дают общее представление о том, как должен выглядеть такой процесс. Есть представление, что термин электронное (цифровое) уголовное дело необходимо закрепить. В своем исследовании И. И. Шереметьев указывает, что «электронное уголовное дело – совокупность процессуальных и иных документов, которые выполнены не в традиционной письменной, а в электронной форме и в порядке, установленном законом» [4. С. 3]. Однако стоит рассматривать электронное уголовное дело, или цифровое уголовное дело в более широком понимании как электронное (с применением цифровых технологий) уголовно-процессуальное производство в целом, а не лишь материальные носители, переведенные в цифровой вид. Ранее в одном из наших исследований уже говорилось, что цифровизация уголовного производства не должна подразумевать «просто дублирование в цифровом виде «бумажного» уголовного дела» [5. С. 167]. Это должен быть инновационно новый подход в производстве расследования с применением цифровых технологий.

Здесь нам ближе видение А. Ф. Абдулвалиева, который придерживается позиции, что электронное уголовное дело по сути это «... программа по формированию уголовного дела, т.е. алгоритм последовательных действий (движения уголовного дела) с момента его возбуждения и до момента исполнения приговора. В числе прочего должны быть предусмотрены бланки и шаблоны отдельных процессуальных документов (например, протокол осмотра места происшествия или протокол предъявления для опознания, графы которых будут заполняться необходимой информацией), что позволит прикреплять к данным документам в электронной форме все сведения о полученных доказательствах, включая фото-, кино- и видеоизображения, а также иные файлы и программные продукты» [6. С. 60]. Р. С. Бурганов указывает, что электронное уголовное дело называть устройством или девайсом необоснованно. В своей статье он приходит к выводу, что со временем переход от бумажного уголовного дела к его электронной форме – это лишь, в определенной степени, изменение технологии фиксации хода расследования, переход от письменного оформления к печатному, типографским способами в дальнейшем, переходу в электронный вид. На наш взгляд, в сегодняшних реалиях уже можно говорить о более серьезном видении электронного уголовного дела. Это должна быть не просто программа, а комплексная государственная информационная система (ГИС), основанная на принципах и требованиях к информационным системам такого рода, в том числе условиям безопасности хранения и обработки данных, доступа к системе участников в зависимости от их процессуального статуса. ГИС «Уголовного дела» будет включать в себя возможности управления через многофункциональное устройство (планшет, КПК, ноутбук или иное портативное устройство), способное к подключению криминалистических средств собирания информации. Такие устройства ускорят процесс приобщения данных расследования к материалам уголовного дела.

Проведенные первичные криминалистические исследования могут быть автоматически внесены в материалы такого уголовного дела. Например, следы на месте происшествия, их идентификация по базам данных будет упрощена.

Осуществление сбора данных при помощи VR-технологий. Создание виртуальных копий места происшествия с применением 3D-сканера позволит визуализировать конкретные места совершения преступления, места производства обыска, выемки, места проведения следственного эксперимента. В устройстве будет отображаться точка места производства следственного действия на основе данных геолокации. В настоящее время описание в текстовом виде с фототаблицами не дает полной картины того, что видел следователь на месте. Также это позволит в деталях рассмотреть данные в дальнейшем в ходе судебного производства данные доказательства. Допросы, проверки показаний на месте, очные ставки, опознания также могут сопровождаться аудио-, видеопотоколированием и вводом записей в систему. Аудиопотоколирование может сопровождаться автоматическим переводом звуковой информации в текстовую, что позволит избежать неправильной трактовки показаний участников следственных действий. Сейчас отдельными учеными-криминалистами уже предлагается набор программ, способных переводить текстовую информацию, записанную «от первого лица» в текст «от третьего лица». Так, в помощь следователям В. А. Воткин и В. А. Пивоваров разработали программный продукт, позволяющий существенно упростить работу следователя в составлении процессуальных документов [7]. Разработанная ими программа учитывает особенности и стилистику текстов подобных процессуальных актов, помогает в составлении постановлений следователя и обвинительного заключения. Таким образом система позволит облегчить работу следственных органов, дознавателей. Достоверность доказательств, собранных и зафиксированных при помощи системы может быть обеспечена строгим соблюдением алгоритмов ввода данных, их хранения и обработки, доступа к устройству лиц с ограниченным перечнем функционала. Например, в системе может быть ограничен доступ к материалам уголовного дела, внесению новых материалов лицами, не включенными в состав следственной группы. Система может предупреждать об истекающих сроках в расследуемом уголовном деле, необходимости обязательных следственных действий, давать подсказки на основе практики расследования схожих дел и аналитике уже ранее расследованных дел, используя методы применения нейросетей. Также система не позволит подменять данные в уголовном деле в дальнейшем. Это обеспечивается за счет использования алгоритмов на основе работы блокчейна. Так, Т. Калентьева и В. Болгова предлагают перевод уголовного дела в цифровой формат на основе технологий блокчейна [8. С. 466]. Все сведения о том, кто входил в систему, когда и какие данные вносил будут проверяемы. Нагрузка на следователей существенно сократится из-за высвобождения времени, затрачиваемого на оформление бумажного материала, составления описи материалов уголовного дела, посещение смежных органов и организаций в целях получения информации.

Говоря о плюсах внедрения уголовного дела, нельзя оставить в стороне проблемы, которые неизбежно сопутствуют любому начинанию. Так анализ проблем внедрения схожих государственных информационных систем показал следующее. В первую очередь это финансирование. В качестве примера можно при-

вести цифры по программе «Электронная Россия (2002–2010 годы)». Согласно документу, на программу за этот период выделялись средства в размере почти 27 миллиардов рублей. Общий объем финансирования программы «Цифровая экономика» в 2024 году составил 25,5 миллиардов рублей [9]. Еще один пример, уже более близкий к теме правовых информационных систем и по стоимости реализации и по воплощению – это ГИС «Правосудие». Финансирование системы в рамках программы «Развитие судебной системы» в 2004–2006 годах потребовало более полутора миллиардов рублей. В последующие периоды затраты росли, на что влияло развитие технологий, замена программного обеспечения иностранного производства на отечественные разработки. Финансирование предполагало создание программного обеспечения, обучение персонала, оплату дополнительных специалистов, приобретение персональных компьютеров и оборудования. Программа развития судебной системы не стоит на месте и требует постоянного финансирования на переоснащение судов и организаций новым оборудованием, создание программного обеспечения (софта) новых сервисов, в том числе в рамках дополнительных ответвлений, таких как «Правосудие онлайн». К примеру, затраты на переоснащение в рамках импортозамещения для Верховного Суда РФ составили 977,5 миллионов рублей в 2024 году. Средства предназначены на закупку более 11 тысяч компьютеров и программного обеспечения российского производства. Стоимость одного комплекта, в который входит компьютер и монитор, по данным опубликованной информации, около 85 тысяч рублей. Как видим затраты на данные проекты достаточно велики. На конец 2022 года предельная численность сотрудников Следственного комитета РФ, при специальных званиях – 20734 человека, а также 2132 человека в военных следственных органах [10]. Конечно, обеспечение каждого сотрудника специальным КПК на первоначальном этапе не понадобится. Помимо самих устройств понадобится вспомогательное оборудование. Оснащение, переобучение, подготовка к работе с системой электронного уголовного дела займет немало средств и времени, однако плюсов от внедрения новой автоматизированной системы все же больше.

Иные проблемы могут носить текущий характер. Так, периодически такие системы подвергаются DDoS-атакам (Denial of Service, «отказ в обслуживании»), они способны блокировать работу системы, приводить к ошибкам в работе. Однако опыт применения уже существующих государственных автоматизированных систем показывает, такие проблемы решаемы. За счет обеспечения систем информационной защитой безопасность может быть обеспечена.

Еще одной проблемой может стать слабая грамотность пользователей системы. Так, если мы подразумеваем, что системой могут пользоваться не профессиональные участники уголовного процесса (потерпевший, свидетель, подозреваемый, обвиняемый и т. д.), то им в первую очередь необходимо будет разъяснять их права пользоваться обычным порядком уголовного судопроизводства. В таком случае следователь, дознаватель, суд обязаны обеспечить возможность выдать в бумажном виде копии процессуальных документов. Однако быстрое внедрение информационных технологий во все сферы жизни человека позволяет освоить навыки использования электронной системы. Наличие самих электронных устройств, через которые они смогут получать информацию, также может стать дополнительной проблемой. Не каждый гражданин может иметь в своем

пользовании смартфон, компьютер. Наиболее важной проблемой остается проблема с доступом к высокоскоростному интернету на территориях, где связь может быть ограничена. Но и эта проблема разрешима. Устройства могут работать в оффлайн-режиме, при необходимости собранная информация может быть передана уже при появлении устройства (КПК) в зоне действия устойчивой связи.

В местах содержания задержанных лиц, а также лиц, находящихся под стражей и в иных учреждениях, необходимо будет предусмотреть возможность использования терминалов, при помощи которых подозреваемый, обвиняемый смогут получать доступ к необходимой информации по уголовному делу. Это также облегчит взаимодействие между следователем или дознавателем с такими лицами.

С целью выяснения мнения непосредственных потенциальных пользователей и участников правоотношений относительно внедрения электронного (цифрового) уголовного дела были проведены беседы со следователями. Выборочный опрос показал, что пока следственные органы настороженно относятся к внедрению инноваций в уголовный процесс. Идет обмен мнениями о внедрении подобной системы в ближнем зарубежье. Коллеги следователей из Казахстана сообщают, что высокую обеспокоенность вызывает сохранность данных, находящихся в материалах уголовных дел, в частности есть риски нарушения тайны следствия. Например, если потерпевшему будет предоставлена возможность получать копии документов в онлайн-режиме через портал «Госуслуги РФ», то логином или паролем для входа в дело воспользуются лица, не являющиеся участниками по уголовному делу. По мнению опрошенных следователей, есть риски утраты самих портативных устройств. И здесь есть предложения по специальной усиленной идентификации должностного лица, которому предоставлено право пользоваться устройством. Иногда следователю намного быстрее и проще составить протокол от руки без применения компьютера. Следователи говорят о рисках сбоев электронных устройств. Все опрошенные согласились с мнением, что уголовное дело должно оставаться и в бумажном виде тоже, но тогда возрастет нагрузка на следователей по оцифровке дела или по его переводу, наоборот, в бумажный вид. Из плюсов, опрошенные указали на то, что внедрение сервисов, связанных с систематизацией уголовного дела, уведомлением по срокам в расследовании дела, составлением простых документов типа описи и шаблонов протоколов, будет полезно. Интегрированные системы с базами данных распознавания личности, идентификация по другим базам и автоматическое внесение в составляемые протоколы такой информации также существенно улучшили бы работу следователей. Опрошенные посетовали на то, что в настоящее время в следственной работе специально для следователей применяется мало компьютерных программ. Апробация внедрения электронного (цифрового) уголовного дела в уголовный процесс на стадии предварительного следствия, по мнению следователей, необходимо пока проводить на менее загруженных уголовными делами следственных отделах, так сказать, в спокойной обстановке. Были предложения проводить апробирование на отделах дознания, где расследуются уголовные дела, не требующие высокой интенсивности от лица ведущего расследования. Это позволит сократить риски дополнительной загрузки, получить достоверные результаты от внедрения системы. Тем не менее, в целом, все

опрошенные приходят к выводу, что если не в ближайшем будущем, то совсем скоро электронное (цифровое) уголовное дело будет не фантастическим, а реальным.

Заключение. Подводя итог, можно сделать вывод, что для создания и внедрения системы электронного уголовного дела уже почти нет препятствий. В скором будущем мы увидим кардинальное развитие уголовного судопроизводства, подкрепленного техническим прогрессом. С положительной стороны стоит оценить перспективы внедрения технологий искусственного интеллекта в уголовно-процессуальном доказывании [11].

Список литературы

1. Концепция цифрового государства и цифровой правовой среды: монография / под общ. ред. Н. Н. Черногора, Д. А. Пашенцева. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: Норма: ИНФРА-М, 2024.
2. Миликова А. В. Требования, предъявляемые к уголовно-процессуальным актам резолютивного характера органов предварительного следствия // Юрист-Правоведь. – 2019. – № 3(90). – С. 78–82.
3. Гимазетдинова И. Н. Уголовное дело как комплексный процессуальный акт и возможность его перевода в электронный формат // Вестник Волгоградской академии МВД России. – 2023. – № 2 (65).
4. Шереметьев И. И. Электронное уголовное дело: Что это такое и пути его создания // LtxRussica. – 2020. – № 10 (167).
5. Малышкин Р. Н. О цифровизации уголовного процесса: актуальные проблемы внедрения электронного уголовного дела // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции: в 6 т., Казань, 22 сентября 2023 года. – Казань: Познание, 2023. – С. 165–170. – EDNNNVHYN.
6. Абдулвалиев А.Ф. Предпосылки и перспективы внедрения электронной формы уголовного дела в деятельность судебных органов // Право и политика. – 2013. – № 1. – С. 59–65.
7. Гармаев Ю. Криминалистика для всех. С подачи следователя-криминалиста, к.ю.н. В. А. Воткина внедряем комп. программу для следователей. URL: https://vk.com/wall-726588_1960
8. Kalenteva T., Bolgova V. Electronic format of criminal cases as a leading trend in modern criminal proceedings // 6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019). – Atlantis Press, 2020. – С. 464–470.
9. Постановление Правительства РФ от 28 января 2002 г. № 65 «О федеральной целевой программе «Электронная Россия (2002–2010 годы)» // Российская Бизнес-газета. 2002. № 6. 12 февраля; 2002. № 7. 19 февраля; 2002. № 8. 27 февраля; Собрание законодательства Российской Федерации. 2002. № 5, ст. 531. URL: <https://base.garant.ru/184120>
10. Указ Президента РФ от 05.12.2022 № 880 «О внесении изменений в Указ Президента Российской Федерации от 14 января 2011 г. № 38 «Вопросы

деятельности Следственного комитета Российской Федерации» // Консультант-Плюс

11. Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. № 1(2). С. 481–497. EDN: acsqxh.

А. Г. Маркелов,

кандидат юридических наук, доцент,
Всероссийский государственный университет
юстиции (РПА Минюста России),
Казанский институт (филиал)

ПРАВО НА ТЕЛЕФОННЫЙ РАЗГОВОР В УГОЛОВНОМ ПРОЦЕССЕ РОССИИ ОСТАЕТСЯ НЕРАЗРЕШЕННОЙ

Аннотация. В статье изложены суждения о новой процессуальной гарантии – предоставление телефонного разговора лицу, задержанного по подозрению в совершении преступления. Показан краткий опыт США, а также отдельные неурегулированные законом проблемы и пути (предложения) по их совершенствованию.

Ключевые слова: телефонный разговор, гарантия, подозреваемый, задержанное лицо, доказательство

THE RIGHT TO TELEPHONE CONVERSATION IN RUSSIAN CRIMINAL PROCEDURE REMAINS UNRESOLVED

Abstract. The article presents some thoughts of the author about a new procedural guarantee – provision of a telephone conversation to a person detained on suspicion of committing a crime. The brief experience of the USA is stated, and also some problems unsettled by the law and ways (proposals) on their improvement are expressed.

Keywords: telephone conversation, guarantee, suspect, detained person, evidence

Федеральным законом от 7 февраля 2011 г. № 3-ФЗ «О полиции» [1] в п. 7 ст. 14 введена процессуальная гарантия, суть которой заключается, в том, что лицо задержанное по подозрению в совершении преступления в кратчайший срок, но не позднее трех часов с момента задержания, если иное не предусмотрено уголовно-процессуальным законодательством РФ, имеет право на один телефонный разговор в целях уведомления близких родственников или близких лиц о своем процессуальном статусе, в том числе сообщить о непосредственном задержании и месте его нахождения. При этом такой телефонный разговор по просьбе задержанного лица могут сделать и сами сотрудники полиции.

Необходимо отметить, что в этом же Федеральном законе в п. 11 ст. 14 определяются исключения, при которых задержанное лицо лишается права на телефонный разговор и уведомление не производится. Таковыми в данном слу-

чае являются лица, совершивших побег из-под стражи, лица, уклоняющихся от отбывания уголовного наказания, от получения предписания о направлении к месту отбывания наказания либо не прибывших к месту отбывания наказания в установленный в указанном предписании срок, – до передачи их соответствующим органам, учреждениям или должностным лицам этих органов и учреждений; лиц, уклоняющихся от исполнения административного наказания в виде административного ареста, – до передачи их в места отбывания административного ареста; лиц, находящихся в розыске, – до передачи их соответствующим органам, учреждениям или должностным лицам этих органов и учреждений; лиц, уклоняющихся от исполнения назначенных им судом принудительных мер медицинского характера или принудительных мер воспитательного воздействия, – до передачи их в учреждения, обеспечивающие исполнение таких мер; лиц, уклоняющихся от следования в специализированные лечебные учреждения для исполнения назначенных им судом принудительных мер медицинского характера, – по основаниям, в порядке и на срок, которые предусмотрены Федеральным законом «О полиции»; лиц, совершивших побег из психиатрического лечебного учреждения или скрывающихся от назначенной судом недобровольной госпитализации в такое учреждение, – до передачи их в психиатрическое лечебное учреждение.

В соответствии с пунктом 14 Наставления о порядке исполнения обязанностей и реализации прав полиции в дежурной части территориального органа МВД России после доставления граждан, утвержденного приказом МВД России от 30 апреля 2012 г. № 389 [2], оперативный дежурный обязан предоставить доставленному и задержанному лицу в кратчайший срок, но не позднее трех часов с момента задержания, если иное не установлено уголовно-процессуальным законодательством Российской Федерации, возможность уведомить близких родственников или близких лиц о факте его задержания и месте нахождения путем осуществления одного телефонного разговора, либо, по просьбе данного лица, произвести указанные уведомления лично, за исключением случаев, которые предусмотрены частью 11 статьи 14 Федерального закона «О полиции». Факт уведомления близких родственников или близких лиц задержанного лица оперативный дежурный обязан отразить в протоколе задержания лица.

Откуда растут корни этой очередной гарантии. Так, похожие по аналогии правовые нормы – например, право задержанного лица на телефонный звонок – имеются и в уголовном судопроизводстве США с 1966 года под оригинальным названием «правило Миранды» [3]. Причиной появления названной процессуальной гарантии, и которое в корне изменило американское уголовное законодательство, послужило фамилия преступника-рецидивиста Эрнесто Артуро Миранды. В его уголовном деле, а точнее в решении, было сказано, что перед началом допроса задержанное лицо должен быть предупрежден о том, что имеет право хранить молчание, при этом оговаривается, что все сказанное им в момент задержания, может быть использовано против него в суде. Кроме этого, у задержанного лица появляется еще одно право на адвоката, который может присутствовать при его допросе. Если же у задержанного лица по каким-

то причинам нет адвоката, либо он не может оплатить его услуги, адвокат будет представлен государством.

Подобные гарантии и соответствующие положения имеются в отдельных штатах США, например, в разделе 851,5 Уголовного кодекса штата Калифорния [4] говорится, что сразу же после ареста, кроме случаев, когда физически невозможно, и не позднее трех часов после ареста, арестованное лицо имеет право сделать три завершенных телефонных звонка. При этом у арестованного лица мобильный телефон сразу отбирается, и звонить арестованному, если и разрешается, то только через специально оборудованный телефон-коммутатор. При предоставлении телефонного звонка лицу, он соединится с оператором правоохранительного органа, который выяснит, куда он хочет позвонить. Оператор проверит названный лицом телефонный номер, в обязательном порядке выясняет у другой стороны, согласны ли там поговорить с вызываемым абонентом и оплатить этот телефонный разговор. При получении положительного ответа и разъяснения последствий такого разговора, произойдет непосредственное соединение, и вся полученная аудиозапись разговора будет зафиксирована. При этом в случае необходимости, записываемая в ходе телефонного разговора информация, может быть использована против задержанного лица, без всяких на то предупреждений, исключение составляет разговор арестованного лица с адвокатом.

Каждый штат США устанавливает свою процедуру предоставления телефонного звонка. Стоит подчеркнуть, например, в штате Миннесоте арестованное лицо имеет право на один телефонный звонок, а не на завершённый разговор, при этом все телефонные разговоры в полиции платные (соединение с абонентом стоит около \$15, минута разговора с абонентом около \$5). Если абонент по каким-то причинам не ответил или будет отказываться от оплаты телефонного звонка, то в данном случае право на телефонный звонок будет признан состоявшимся [5].

Что происходит на этот счет в нашей стране. В Российском уголовном процессе, в частности Федеральным законом от 30.12.2015 № 437-ФЗ [6] были внесены дополнения в Уголовно-процессуальный кодекс Российской Федерации (далее – УПК РФ) [7], которые предоставляют задержанному лицу право на один телефонный разговор с момента доставления его к следователю или в орган дознания. До указанного события по российскому уголовно-процессуальному законодательству у задержанных по подозрению в совершении преступления лиц такой возможности не было. Сформулированная гарантия предоставлялась только тем лицам, которые были задержаны сотрудниками полиции в соответствии с Федеральным законом «О полиции», вступившим в силу с 01 марта 2011 года. Таким образом, законодательное нововведение в действующий УПК РФ существенно уравнило в правах всех лиц, задерживаемых правоохранительными органами.

В соответствии с внесенными изменениями в ч. 1 ст. 96 УПК РФ, подозреваемое лицо в кратчайший срок, но не позднее 3 часов с момента его доставления в орган дознания или к следователю, имеет право на один телефонный разговор на русском языке в присутствии дознавателя, следователя в целях уведомления близких родственников, родственников или близких лиц

о своем задержании и месте нахождения, о чем делается отметка в протоколе задержания.

В прежней редакции федерального закона дознаватель, следователь не позднее 12 часов с момента задержания подозреваемого уведомлял кого-либо из его близких родственников, а при их отсутствии – других родственников или предоставлял такую возможность самому подозреваемому лицу. Если подозреваемое лицо откажется от такого права на телефонный разговор, или в силу физических или психических недостатков не сможет самостоятельно осуществлять свое право, такое уведомление будет произведено дознавателем, следователем, о чем также делается отметка в протоколе задержания.

При этом законодатель в части 4 указанной статьи специально установил, что при необходимости сохранения в интересах предварительного расследования в тайне факта задержания уведомление родственникам и близким лицам по мотивированному постановлению дознавателя, следователя с согласия прокурора может не производиться. Исключение составит случаи, когда подозреваемое лицо является несовершеннолетним.

Необходимо акцентировать внимание на то обстоятельство, что изложенная редакция Федерального закона расширяет круг лиц, кому может позвонить подозреваемый. Таким образом, задержанное лицо имеет право на телефонный разговор с любым человеком, которого он считает близким лицом, включая и защитника (адвоката).

А теперь сформулируем процессуальные проблемы реализации этой гарантии. К сожалению, законодатель не устанавливает и не поясняет процессуальный порядок предоставления подозреваемому лицу права на телефонный разговор, не указывает механизм фиксации сведений, изложенных в телефонном разговоре, а также возможные негативные последствия такого разговора. Сообщенные в телефонном звонке сведения подозреваемым могут «плачевно» скажаться на раскрытии преступления, в том числе и на возможное уничтожение следов преступления, и, наоборот, в свою очередь могут иметь и доказательственное значение виновности лица, подозреваемого в совершении преступления. Более того, получив такую гарантию, задержанное лицо может попытаться раскрыть какие-либо сведения о предварительном расследовании на своем родном языке, например, когда, если разговор ведется на языке, которым следователь, дознаватель не владеет. Необходимо законодательно закрепить процедуру последствий таких разговоров в виде разъяснения прав и обязанностей подозреваемого. Считаем необходимым отметить, что если лицо изъявил желание позвонить своему близкому человеку, то он в обязательном порядке должен быть предупрежден о последствиях такого ходатайства. В любом случае все сообщенные им сведения будут записаны на аудио- или видеоноситель и они при возникновении проблемной ситуации могут быть использованы в качестве доказательств по уголовному делу, в том числе и при его последующем отказе.

Кроме того, до сих пор законодатель не определил, что считать моментом доставления подозреваемого в органы дознания или предварительного следствия, и не уточняет конкретный срок, в который подозреваемый должен предстать перед дознавателем или следователем после своего задержания. В этой связи считаем необходимым предложить законодателю, а в дальнейшем и право-

применительно предоставлять такое право лицу, задержанного по подозрению в совершении преступления с момента составления протокола задержания.

Остается еще одна важная проблема, которую законодатель в этой части не отрегулировал. Так, сохраняется не разрешенной аналогичная ситуация с лицом, в отношении которого избрана или принято процессуальное решение о продлении срока пребывания под стражей. В этой связи считаем необходимым дополнить часть 12 статьи 108 УПК РФ соответствующими положениями, аналогичной по своей конструкции статьи 96 УПК РФ.

Таким образом, правовой институт задержания подозреваемого лица в уголовном процессе в виде очередной гарантии – предоставление телефонного разговора нуждается в дальнейшем совершенствовании, исключив возможность применения правоприменителем неверных действий. Предприняв очередную попытку расширения прав задержанного по подозрению в совершении преступления лица, законодатель, по нашему мнению, оказался далек от его оптимального воплощения.

Список литературы

1. О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 7, ст. 900.
2. Об утверждении Наставления о порядке исполнения обязанностей и реализации прав полиции в дежурной части территориального органа МВД России после доставления граждан: приказ МВД России от 30.04.2012 г. № 389 // Рос. газ. 2012. 11 июля.
3. Правило Миранды. История рецидивиста, изменившего американское правосудие [Электронный ресурс]. URL: <http://www.aif.ru/society/law/1309898> (дата обращения: 30.06.2024).
4. Калифорнийский Уголовный кодекс [Электронный ресурс]. URL: <http://ru.encydia.com> (дата обращения: 30.06.2024).
5. Уголовное законодательство штата Миннесота [Электронный ресурс]. URL: <http://pravo.ru>.
6. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 30.12.2015 № 437-ФЗ // Рос. газ. 2016. 11 янв.
7. Уголовно-процессуальный кодекс Российской Федерации // Рос. газ. 2001. 22 дек.

И. Э. Никитина,
доктор юридических наук, профессор,
Российский университет транспорта;
главный научный сотрудник,
Российский федеральный центр судебной экспертизы
имени профессора А. Р. Шляхова
при Министерстве юстиции Российской Федерации

ВЗАИМОДЕЙСТВИЕ ГОСУДАРСТВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И ПРАВА ЧЕЛОВЕКА

Аннотация. В статье анализируются правовые проблемы взаимодействия государств при расследовании преступлений, совершенных с использованием современных информационно-коммуникационных технологий и права человека в эпоху цифровых технологий. Дан прогноз по возрастанию глобальных расходов на кибербезопасность. Рассматриваются позиции правоохранительных органов и основателей социальных сетей по вопросам внедрения таких технологий, как сканирование на стороне клиента для обнаружения противозаконного контента. Обосновывается то, что защита конфиденциальной информации является важнейшим приоритетом, поскольку государства продолжают сталкиваться с растущим числом утечек данных и более строгими требованиями к соблюдению требований.

Ключевые слова: информационно-коммуникационные технологии, искусственный интеллект, социальные сети, взаимодействие государств, Павел Дуров, Франция, законодательство ЕС, Суд Европейского Союза

INTERACTION BETWEEN STATES TO INVESTIGATE CRIMES COMMITTED USING MODERN INFORMATION AND COMMUNICATION TECHNOLOGIES AND HUMAN RIGHTS

Abstract. The article analyzes the legal issues of interaction of states in the investigation of crimes committed using modern information and communication technologies and human rights in the digital age. A forecast is given for the increase in spending on cybersecurity. The positions of external bodies and founders of social networks on issues of such technologies as scanning on the side, necessary for the detection of illegal content, are considered. It is substantiated that the protection of confidential information is the most important priority, as the state continues to face an increasing number of data leaks and stricter requirements for compliance.

Keywords: information and communication technologies, artificial intelligence, social networks, interaction of states, Pavel Durov, France, EU legislation, Court of Justice of the European Union

Введение. С появлением информационно-коммуникационных технологий мировому сообществу потребовалось как защищать электронные данные, так

и получать доступ к ним при расследовании преступлений в сфере высоких технологий [2].

Тем не менее довольно остро встают проблемы пределов допустимости средств и методов получения доказательств на территориях иностранных государств. В директиве Европейского союза 2014/41/ЕС о сотрудничестве государств по уголовным делам предусмотрен единый инструмент – Европейский следственный ордер (ЕЮ) по уголовным делам в целях получения доказательств, уже находящихся в распоряжении компетентных органов исполняющего решение государства.

Ордер используется в тех случаях, когда выполнение следственного действия обоснованно предполагается соразмерным, адекватным и применимым к рассматриваемому делу [1].

Тем не менее вопрос о правомерности использования доказательств из зашифрованных телефонных сетей граждан одной страны, в которые проникли правоохранительные органы другой страны, был рассмотрен Судом Европейского Союза (СЈЕУ) [4].

Основная часть. В своем решении от 30 апреля 2024 года Суд ЕС постановил, что государства-члены должны официально уведомлять другие государства-члены, когда они перехватывают сообщения, находящиеся под их юрисдикцией.

Ожидается, что решение высшего суда ЕС приведет к судебным разбирательствам по поводу использования доказательств из EncroChat и других зашифрованных телефонных сетей, в которые проникли правоохранительные органы. EncroChat – провайдер коммуникационных сетей и услуг, базировавшийся в Нидерландах. По данным полиции, мессенджер EncroChat использовали члены многих организованных преступных группировок для планирования преступных действий. Сервис EncroChat представляет собой мобильное устройство на базе ОС Android, в котором были отключены функции геолокации, встроенной камеры и микрофона, а также были внесены изменения в ОС, препятствующие внедрению бэкдоров и иных средств негласной слежки.

В ходе расследования, проведенного французскими властями, выяснилось, что обвиняемые использовали зашифрованные мобильные телефоны, работающие по лицензии «EncroChat», для совершения преступлений, в первую очередь связанных с незаконным оборотом наркотиков.

С разрешения судьи французская полиция смогла получить данные с этого сервера в 2018 и 2019 годах. Эти данные позволили совместной следственной группе, в которую вошли эксперты из Нидерландов, разработать часть троянского программного обеспечения. Весной 2020 года с разрешения Уголовного суда (Лилль, Франция, Tribunal correctionnel de Lille) данное программное обеспечение было загружено на сервер, а оттуда установлено на мобильные телефоны с помощью симулированного обновления. Из 66 134 тысяч подписанных пользователей 32 477 пользователей в 122 странах пострадали от этого программного обеспечения, в том числе около 4 600 пользователей в Германии. Операция привела к 6500 арестам по всему миру и конфискации почти 900 миллионов евро после трехлетнего расследования, проведенного полицией в отношении органи-

зованной преступности и наркогруппировок, использующих возможности EncroChat.

Однако, Франция не предоставила Германии и другим государствам-членам официального уведомления о хакерской операции, как того требует законодательство ЕС, таким образом Франция «нарушила закон». Согласно директиве 2014/41/ЕС Франция была обязана официально уведомить Германию о прослушивании телефонов EncroChat на немецкой территории и предоставить немецким властям возможность возразить против операции в течение 96 часов.

Уведомление от Франции должно было содержать подробную информацию о целях операции, номерах телефонов, IP-адресах или электронных почт, личностей преследуемых лиц, включая их адрес, дату рождения и номера социального страхования, а также описание совершенного преступления, согласно образцу уведомления, включенного в директиву 2014/41/ЕС.

Согласно уголовно-процессуальному законодательству Германии данные, собранные посредством прослушивания телефонных разговоров – при отсутствии судебного одобрения и при отсутствии конкретных подозрений в конкретном правонарушении – считаются недопустимыми.

Согласно прецедентному праву ЕС, борьба с тяжкими преступлениями не может служить оправданием всеобщего и неизбирательного хранения персональных данных.

Решение Суда ЕС. Государственный прокурор в Германии может выдать Европейский следственный ордер для получения доказательств, полученных, скажем, во Франции, путем перехвата сообщений в Германии, при условии, что Европейский следственный ордер удовлетворяет всем условиям, изложенным в немецком законодательстве для передачи аналогичных доказательств в Германии.

Франция должна уведомить Германию, если она перехватывает телекоммуникации на территории Германии. Информация, требуемая в уведомлении, изложена в директиве 2014/41/ЕС.

Европейский следственный ордер (согласно статье 31 директивы 2014/41/ЕС) также предназначен для защиты прав людей, подвергающихся перехвату телекоммуникаций.

Согласно французскому законодательству, операторы зашифрованных услуг связи могут быть оштрафованы, приговорены к тюремному заключению или конфискованы без получения официального разрешения.

Правоохранительные органы и правительства оказывают давление на сервисы зашифрованных сообщений, требуя внедрения таких технологий, как сканирование на стороне клиента для обнаружения противозаконного контента.

Основатель Telegram Павел Дуров был задержан французской полицией в ходе операции, инициированной Центром жандармерии по борьбе с киберпреступностью (C3N) и Национальным управлением по борьбе с мошенничеством (ONAF).

Его обвиняют в не сотрудничестве с правоохранительными органами по запросам о законном перехвате. Сервис предоставляет возможность зашифрованного обмена сообщениями с использованием «секретных чатов». В отличие от других приложений для зашифрованных сообщений, таких как Signal или WhatsApp, шифрование не включено по умолчанию.

Он также позволяет обмениваться сообщениями в группах численностью до 200 000 человек и транслировать материалы по каналам для большой аудитории.

Заключение. Согласно прогнозу Gartner, в 2025 глобальные расходы на кибербезопасность вырастут на 15% году благодаря Искусственному интеллекту.

Значительная часть этого роста связана с тем, что внедрение искусственного интеллекта (ИИ) и, в частности, генеративного ИИ (GenAI) становится все более распространенным, что требует инвестиций в безопасность приложений, безопасность данных, меры по обеспечению конфиденциальности и защиту сетевой инфраструктуры [3].

Что касается конфиденциальности и защиты данных, то наиболее заметными сферами инвестиций станут безопасность электронной почты, конфиденциальность и управление данными, управление уязвимостями, тестирование на проникновение и предотвращение потери данных (DLP), оценка рисков, а также шифрование данных и криптография.

Значительные инвестиции в DLP, безопасность электронной почты, конфиденциальность и управление, по-видимому, указывают на то, что защита конфиденциальной информации является важнейшим приоритетом, поскольку государства продолжают сталкиваться с растущим числом утечек данных и более строгими требованиями к соблюдению требований.

Аль-Фараби отмечал, что достойное международное сотрудничество может быть реализовано только в том случае, если государства будут сотрудничать ради безопасности всего человечества, его счастья и благополучия.

Сегодня преступность представляет собой одну из самых сложных проблем современного мира, не знающую границ и преград. Это социальное явление транснационального характера, которое грозит уничтожить общечеловеческие ценности человеческой цивилизации. Организованная преступность, терроризм и другие серьезные формы преступности сегодня являются глобальной проблемой номер один, и борьба с ними требует солидарности, сотрудничества и участия всего международного сообщества [5].

Список литературы

1. Бирюков, Павел Н. 2019. «Имплементация в государствах – членах Европейского союза правил о Европейском следственном ордере». Вестник Санкт-Петербургского университета. Право 3: 566–576.

<https://doi.org/10.21638/spbu14.2019.311>

2. Климова Я. А. Искусственный интеллект и цифровые доказательства в расследовании преступлений, совершенных с использованием современных информационно-коммуникационных технологий // Вестник Волгоградской академии МВД России. 2023. № 1 (64). С. 81–87. doi: 10.25724/VAMVD.A079

3. Решение Суда Европейского Союза (Большой Палаты) 30 апреля 2024 г. Информационный ресурс: URL:

<https://curia.europa.eu/juris/document/document.jsf?jsessionid=5EDB351DDD0DDE5161E78AD026B29472?text=&docid=285365&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=251571> (дата обращения: 02.09.2024.)

4. Информационный ресурс: URL:
https://www.computerweekly.com/news/366609115/Global-cyber-spend-to-rise-15-in-2025-pushed-along-by-AI?utm_campaign=20240829_Telegram+founder+Pavel+Durov+questioned+over+cyber+crime+charges&utm_medium=email&utm_source=MDN&source_ad_id=366609115&asrc=EM_MDN_301110376&bt_ee=topHUuCcRvkxps50A4fzlHLpP5igX8UKBQ%2FwcNUAfnGKNe01Gb0Vao5miX6WKwjO&bt_ts=1724927384653 (дата обращения: 02.09.2024.)

5. Željko NIKAČ, Branko LEŠTANIN. The importance of international police cooperation for the balanced positioning of Serbia in contemporary international relations // International Organizations: Serbia and Contemporary Vol. 2 / Duško Dimitrijević, Toni Mileski (Eds.). – Belgrade : Institute of International Politics and Economics ; Skopje : Faculty of Philosophy of the University of St. Cyril and Methodius, 2022 (Belgrade : Donat Graf). 530 str.

А. А. Петрикина,
кандидат юридических наук, доцент,
Российский государственный университет правосудия,
Северо-Кавказский филиал

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ СУДЕБНОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. На основе научного анализа отдельных видов деятельности судов определяются основные проблемы внедрения цифровых технологий в данной сфере. Предложенные пути их решения существенно помогут в осуществлении правосудия и реализации судами иных функций, ведь применение цифровых технологий всегда должно приводить к повышению качества жизни граждан в нашей стране.

Ключевые слова: суд, цифровые технологии, судебная система, искусственный интеллект, права человека, правосудие, судебное решение

DIGITAL TECHNOLOGIES IN THE ACTIVITIES OF THE JUDICIAL SYSTEM OF THE RUSSIAN FEDERATION

Abstract. Based on the scientific analysis of certain types of court activities, the main problems of the introduction of digital technologies in this area are determined. The proposed solutions will significantly help in the administration of justice and the implementation of other functions by the courts, because the use of digital technologies should always lead to an improvement in the quality of life of citizens in our country.

Keywords: court, digital technologies, judicial system, artificial intelligence, human rights, justice, judicial decision

Введение. Цифровые технологии в рамках судебной системы Российской Федерации развиваются динамично и сложно из-за особой важности исследуе-

мой структуры государственной власти. Современное состояние судебной системы, происходящие процессы по оптимизации ее правовой регламентации, имеющиеся пробелы в нормативно-правовых актах, организационные трудности при осуществлении правосудия свидетельствуют о потребности своевременного и четкого формулирования наиболее актуальных проблем, требующих незамедлительного реагирования научного сообщества, законодательных органов, правоприменителей для определения основных векторов дальнейшего реформирования [5. С. 245–246], особенно в сфере новых технологий. Решение проблемных вопросов развития судебной системы необходимо для успешного существования гражданского общества [3. С. 100] и правового государства.

Основная часть. Сегодня выделяют ряд проблем в работе судебной системы [4. С. 153]. Среди них особое место занимают такие, как загруженность судов, что негативно сказывается на судопроизводстве; человеческий фактор при отборе судейских кадров, их недостаточная подготовленность в плане владения высокими технологиями; дефицит работников судебной системы, оказывающих содействие осуществлению правосудия, сложность судебной статистической отчетности.

Именно в данных направлениях нужно активно использовать искусственный интеллект, специально разработанные цифровые платформы и компьютерные программы.

Роль и место в судебной системе мировой юстиции, ее загруженность, обеспечение независимости мирового судьи от региональных органов власти и должностных лиц, налаживание эффективной работы аппарата мирового судьи на единых принципах, началах и равном уровне финансирования с федеральными судами, а также обеспечении надлежащего материально-технического снабжения также можно решить при помощи современных цифровых технологий.

Конечно, для начала нужно улучшить нормативное регулирование деятельности мировых судов, необходимо разработать новые способы организации их деятельности с использованием искусственного интеллекта, определив критерии допустимости работы с ним в данной сфере. Кроме того, необходимо не только определить и закрепить место цифровых технологий в судебной системе РФ [2. С. 105], но и привести в соответствие в этом плане законодательство, регулирующее деятельность мирового суда и правовой статус судьи.

В ближайшей перспективе специализированные суды должны быть наделены особой компетенцией и иметь инновационное регулирование с учетом стремительно развивающихся цифровых технологий [8. С. 210].

Осторожное включение в их деятельность искусственного интеллекта будет способствовать совершенствованию правосудия по делам об отстаивании авторских прав. Данный фактор активно будет способствовать приближению осуществления правосудия к населению, повышению и улучшению качества судебных решений [9. С. 16; 10. С. 1284].

Не лишенным рациональности видится создание системы специализированных судов на всей территории государства. Законодателю стоит разграничить подсудность специализированных судов и иных судов, установив закрытый перечень рассматриваемых дел, которые должны быть им подсудны, ввести, например, на платформе «Государственные услуги», обязательное информирова-

ние граждан при обращении в такие суды, содержащее сведения о конкретных направлениях защиты прав лиц.

Рассмотрим в рамках Суда по интеллектуальным правам возможность решить с помощью цифровых технологий проблему нехватки сведующих лиц в целях их привлечения в судебный процесс. Например, можно создать электронный реестр лиц, обладающих специальными знаниями для данной категории дел, разработать специальную программу, которая бы исключала влияние человеческого фактора при выборе специалиста/эксперта.

До сих пор очень сложным остается вопрос использования цифровых технологий при осуществлении правосудия [1. С. 98], представляющего собой уникальную комплексную деятельность органов судебной системы Российской Федерации по рассмотрению гражданских, арбитражных, административных и уголовных дел в целях защиты нарушенных прав человека и гражданина на основе строго определенных легальных правил.

Правосудие представляет собой особый специфический институт государственной власти – одну из ее основных сфер (наравне с законодательной и исполнительной властью) и охватывает почти все сферы жизнедеятельности общества

Одной из угроз формирования прозрачной судебной системы и совершенствование доступности правосудия видится коррупция. Бороться с этим негативным социальным явлением во многом также можно за счет цифровых технологий, осуществлять:

контроль с помощью искусственного интеллекта за принципиально новыми средствами электронного платежа (криптовалюта/цифровой рубль);

наладить общую совместную работу правоохранительных органов и антикоррупционных государственных органов и организаций на базе единой цифровой платформы;

повышение уровня правовой культуры населения, посредством формирования системы непрерывного антикоррупционного образования на базе платформы «Государственные услуги».

Заключение. Подводя итоги, стоит отметить, что современная отечественная судебная система в рамках действующего законодательства предусматривает широкий спектр правовых гарантий участников судебного процесса, которые, по буквальному своему смыслу, должны исключать случаи необоснованного ограничения конституционных прав граждан. Тем не менее последние достижения научно-технического процесса до сих пор не учтены в судопроизводстве должным образом.

Таким образом, необходимо принять скорее ФКЗ «О цифровых технологиях в судебной системе РФ», а также внести в связи с этим отдельные поправки в УПК РФ, АПК РФ, КАС РФ, ГПК РФ, это позволит сделать правосудие в России более доступным, открытым и независимым.

Список литературы

1. Брянцева О. В., Солдаткина О. Л. Электронное правосудие в России: проблемы и пути решения // Вестник ун-та им. О. Е. Кутафина (МГЮА). – 2019. – № 12 (64). – С. 97–98.

2. Добровлянина О.В. Внедрение новых электронных технологий в уголовное судопроизводство // *Ex iure*. – 2019. – № 2. – С. 104-117.
3. Карасев А. Т. Цифровизация правоотношений и ее влияние на реализацию отдельных конституционных прав граждан в Российской Федерации // *Антиномии*. – 2019. – № 3. – С. 99–119.
4. Малько А. В. Проблемы цифровизации в сфере осуществления правосудия // *Государство и право*. – 2020. – № 10. – С. 151–159.
5. Приженникова А. Н. Цифровизация правосудия: теоретические и практические аспекты // *Образование и право*. – 2020. – № 2. – С. 240–250.
6. Солдаткина О. Л. Проблемы формирования понятийного аппарата концепции цифровизации правосудия // *Информационное право*. – 2020. – № 3. – С. 23–27.
7. Софийчук Н. В. К вопросу о доступе граждан к правосудию в условиях цифровизации судопроизводства // *Lexrussia (Русский закон)*. – 2020. – № 11(168). – С. 71–80.
8. Чурикова А. Ю. Проблемы цифровизации российского уголовного процесса // *Вестник СГЮА*. – 2021. – № 6(143). – С. 209–216.
9. Broomhall B. *International Justice and the International Criminal Court: Between Sovereignty and the Rule of Law*. Oxford: Oxford Univ. Press, 2003, p. 16.
10. Dutton Y. *Virtual Witness Confrontation in Criminal Cases: A Proposal to Use Videoconferencing Technology in Maritime Piracy Trials*. *Vanderbilt Journal of Transnational Law*, 2012, no. 5, pp. 1283–1340.

П. К. Петров,

кандидат юридических наук, доцент,
Южно-Уральский государственный университет
(национальный исследовательский университет)

ЦИФРОВИЗАЦИЯ УГОЛОВНОГО СУДОПРОИЗВОДСТВА: ПРОБЛЕМЫ ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ

Аннотация. В процессе расследования уголовных дел чаще всего возникает вопрос о сокращении сроков по делу. Это касается и сроков предварительного следствия и сроков дознания. Однако не всегда есть возможности разрешить этот вопрос максимально эффективно, соблюдая все права и свободы человека и гражданина. Использование достижений науки и техники, искусственного интеллекта, цифровых технологий позволяет работать более качественно, быстро, собирать доказательства тщательно и сокращать процессуальные расходы. Тем не менее сам процесс цифровизации уголовного судопроизводства на сегодняшний день достаточно тяжело проходит по ряду объективных и субъективных причин. Именно изучения эти причин посвящена данная статья.

Ключевые слова: электронные доказательства, цифровые доказательства, уголовное судопроизводство, дознание, предварительное следствие, процессуальные сроки

DIGITALISATION OF CRIMINAL PROCEEDINGS: PROBLEMS OF LAW ENFORCEMENT PRACTICE

Abstract. In the process of investigation of criminal cases, the question of shortening the time limits in the case most often arises. This applies to the terms of preliminary investigation and terms of enquiry. However, it is not always possible to resolve this issue as efficiently as possible, observing all the rights and freedoms of man and citizen. The use of achievements of science and technology, artificial intelligence, digital technologies allows to work more qualitatively, quickly, collect evidence thoroughly and reduce procedural costs. Nevertheless, the very process of digitalisation of criminal proceedings is currently quite difficult for a number of objective and subjective reasons. This article is devoted to the study of these reasons.

Keywords: electronic evidence, digital evidence, criminal proceedings, enquiry, preliminary investigation, procedural terms

Введение. В практике приходится работать с большим количеством данных. Участники уголовного процесса могут пользоваться широким спектром возможностей, что отражается на объемах дел, их многотомности. Стороны иногда злоупотребляют своим правом и приобщают к материалам дела информацию, которая имеет косвенное отношение к сути доказывания, но, в связи с тем, что следователь или дознаватель, а также сам защитник или даже судья опасаются жалоб и конфликтности в процессе, все-таки приобщают данные документы («пустые» по своей сути), что увеличивает объем самого материала. Оцифровка такого дела займет много времени, много сил для архивирования данных и их аналитической обработки. Несомненно, это одна из ключевых проблем цифровизации современного уголовного судопроизводства [4]. Если рассматривать эту проблему только со стороны электронных доказательств, то можно выбрать форму электронного документа и на этом закончить работу, однако, современные тенденции реформирования уголовно-процессуального закона такими действиями не ограничиваются. В процессе расследования уголовного дела должны быть собраны необходимые доказательства, относящиеся к событию преступления, а также к характеристике обвиняемого и потерпевшего.

Основная часть. Для того чтобы оцифровать материалы необходимо огромное количество ресурсов, технологий и денежных средств. Цель, которую преследуют при оцифровке – документы, визуальные копии вещественных доказательств, которые полностью равнозначны между собой и соответствуют оригиналу.

Еще одной особенностью уголовного процесса является презумпция невиновности обвиняемого, гарантированная как Конвенцией о защите прав человека и основных свобод, так и основными законами большинства государств. Презумпция не только напрямую влияет на бремя доказывания, но и существенно ужесточает правила оценки каждого отдельного доказательства: суду необходимо проследить всю цепочку досудебного получения и хранения доказательства.

Оцифровка позволяет достичь еще одного уровня повышения эффективности процесса: судье предстоит дать правовую оценку оцифровке данных. Само

доказательство не должно измениться, по существу, документы должны быть одинаковыми по содержанию. Безусловно возникает двойственная ситуация: с одной стороны, суд должен стать основой правовой мысли, но при этом, он же может допустить роковую ошибку при вынесении решения.

Основными преимуществами при цифровизации являются: повышение эффективности судебных заседаний, сокращение сроков судебных заседаний, ускорение электронного документооборота. Возможным также становится устранить задержки в судебных процессах, долгие перерывы между судебными заседаниями. Тем не менее, остается открытым вопрос, о том, как наладить работу судов и следственных изоляторов и исправительных колоний, чтобы не было допущено срывов судебных заседаний.

Важным является обеспечить участникам уголовного судопроизводства доступ к необходимым материалам и документам в режиме реального времени, что способствует более оперативному принятию решений. Цифровизация позволяет устранить быстро географические и финансовые ограничения для участников судебного процесса. Благодаря возможности проведения видеоконференций стороны могут участвовать в судебных заседаниях без необходимости физического присутствия в зале суда. Важно обеспечить суд качественной техникой и высокоскоростным интернетом. Далее дело остается за малым. Научить сотрудников пользоваться этими материалами.

Цифровой формат документов и электронное хранение данных способствуют сохранности информации, исключая возможность случайного уничтожения или повреждения. Кроме того, с использованием цифровых подписей и шифрования можно обеспечить конфиденциальность и неприкосновенность юридически значимых документов. Цифровизация позволяет сократить расходы на бумажные документы, доставку почты и другие традиционные процессы, связанные с бумажной работой. Это позволяет оптимизировать ресурсы и сократить издержки судебной системы. Необходимо сократить все процессы, связанные с резервным копированием в бумажном виде материалов, которые существуют в цифровом виде. При этом важно подчеркнуть и возможные вызовы и ограничения цифровизации уголовного судопроизводства. К наиболее важным свойствам относятся: сохранность и безопасность данных, непрерывность обмена информацией, досудебная подготовка процесса, правовые и этические вопросы [3].

Традиционно по делам публичного обвинения (а подавляющее большинство уголовных дел относятся именно к ним) доказательства начинают собираться, а дело – формироваться на этапе предварительного расследования. В зависимости от страны в предварительном расследовании задействуются полиция, отдельный следственный орган, прокуратура или все они вместе. Соответственно, возрастает и число цифровых аватаров человека (если рассматривать, например, виртуальный судебный процесс), между которыми уголовное дело может передаваться для принятия процессуальных решений. Уже на стадии предварительного расследования могут появиться полиция, следователь, прокурор, обвиняемый, потерпевший, свидетель, гражданский истец и ответчик. И только затем следует судебная стадия, на которой часть субъектов предварительного расследования исчезает [1. С. 55].

Заключение. Уголовное судопроизводство представляет собой предварительное расследование и дознание, в ходе которых информация и доказательства могут собираться и представляться между большим количеством субъектов – участников уголовного судопроизводства. Для цифровизации уголовного процесса требуется большое количество ресурсов и финансирования, однако эти процессы должны быть завершены в ближайшее время.

Список литературы

1. Андреева И. А. На пути к радикальной полицейской реформе Франции. Объединение национальной полиции и национальной жандармерии // Научный вестник Омской академии МВД России. 2011. № 4(43). С. 55–59.
2. Бродовски Д., Ян М. Цифровые доказательства в немецком уголовном процессе на стадиях предварительного расследования, рассмотрения дела по существу и ревизии // Российское право: образование, практика, наука. 2020. № 3. С. 4–19.
3. Лонская С. В. Цифровая история права: принципы методологии // Цифровые технологии и право. 2024;2(1):14–33. <https://doi.org/10.21202/jdtl.2024.2>
4. Проскурякова М. И. Электронное правосудие в Германии: актуальное состояние и перспективы развития // Вестник Санкт-Петербургского университета. Право. 2018. Т. 9, вып. 3. С. 433–447.
5. Уголовный процесс европейских государств: моногр. / В. В. Луцик, А. Б. Войнарович, В. А. Савченко [и др.]. М.: Проспект, 2018. 752 с.
6. Пучковская А. А., Зимина Л. В., Волков Д. А. Введение в цифровые гуманитарные исследования: учебно-методическое пособие. Санкт-Петербург: Университет ИТМО, 2021.

П. К. Петров,

кандидат юридических наук, доцент,
Южно-Уральский государственный университет
(национальный исследовательский университет)

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ И ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В МЕТОДИКЕ ЗАЩИТЫ ПО УГОЛОВНЫМ ДЕЛАМ

Аннотация. Современная теория правоприменительной практики такова, что при расследовании преступлений возникает масса сложностей, связанных с фиксацией тех или иных следов с использованием современных технологий и технических средств, кроме того, с возникновением нового круга общественных отношений – информационных и цифровых, возникает необходимость зафиксировать данные цифрового с электронных и цифровых ресурсов. Поскольку институт адвокатуры является смежным по отношению к общепринятой системе правоохранительных органов Российской Федерации, адвокатам зачастую трудно работать с электронными и цифровыми ресурсами, запрашивать их в качестве доказательств невиновности своих подзащитных, а также решать оперировать ими в суде. Сущности электронных и цифровых доказательств в деятельности адвокатов посвящена представленная статья.

Ключевые слова: электронные доказательства, цифровые доказательства, адвокат, защита по уголовным делам, квалификация преступлений, защита прав обвиняемого, защита прав потерпевшего

USE OF DIGITAL AND ELECTRONIC EVIDENCE IN THE DEFENCE OF CRIMINAL DEFENCE METHODOLOGY

Abstract. The modern theory of law enforcement practice is such that during the investigation of crimes a lot of difficulties arise related to the fixation of certain traces with the use of modern technologies and technical means, moreover, with the emergence of a new range of social relations – information and digital, there is a need to fix the data of digital from electronic and digital resources. Since the institution of advocacy is adjacent to the generally accepted system of law enforcement agencies of the Russian Federation, it is often difficult for lawyers to work with electronic and digital resources, to request them as evidence of innocence of their clients, and to decide to operate them in court. The presented article is devoted to the essence of electronic and digital evidence in the activity of lawyers.

Keywords: electronic evidence, digital evidence, lawyer, criminal defence, qualification of crimes, protection of the rights of the accused, protection of the rights of the victim

Введение. В 2018 году в уголовно-процессуальный закон были внесены существенные изменения, изменившие судебную и следственную практику. В законе появилась специфика описания изъятия электронных носителей информации и копирования с них информации при производстве следственных действий, в том числе устанавливает обстоятельства, при которых вполне возможно и законно изъять информацию следователем в ходе производства следственного действия, которая важна для уголовного дела. Также указывается роль специалиста при всех вышеназванных процессуальных действиях, однако нет сведений о том, какую роль будет занимать адвокат в этом процессе. Основной проблемой в данном случае видится отсутствие разграничений между электронными и цифровыми доказательствами, а, следовательно, формами их закрепления и изъятия всеми участниками процесса, которые полномочны на это.

Основная часть. Многие следователи-криминалисты на практике при работе с доказательствами по-прежнему отождествляют электронные доказательства и цифровые, а также доказательства, форма которых была изменена с бумажного в электронный или цифровой формат. Для адвокатов такие сведения еще более сложны в понимании, поскольку многие технические вопросы остаются неизвестными.

По данным МВД, число IT-преступлений в России в 2023 году увеличилось почти на 30%. Вместе с этим выросло и желание граждан обезопасить себя. За прошлый год россияне более 28 тыс. раз обращались к нотариусам, чтобы зафиксировать нарушение их прав в цифровом пространстве [1, с. 118].

Так, Ю. В. Шелегов и В. Г. Шелегов [5. С. 65] отождествляют понятия «электронное» и «цифровое» доказательство, относят их к категории «электронные документы», которые квалифицируются как «вещественные доказательства и как иные документы (в случае если текстовые электронные документы содер-

жат реквизиты)». Такая точка зрения встречает множество вопросов при обсуждении, поскольку доказательство и документ – это не одно и то же, а электронный документ и цифровой документ – это совершенно разные понятия. Смещение терминов свойственно авторской позиции В. Н. Чернышова, Е. С. Лоскутовой: «...одним из требований, предъявляемых к электронным доказательствам, является то, что цифровые носители информации, скопированные или полученные с других носителей в ходе производства следственных действий, должны быть приложены к протоколу соответствующего следственного действия, о чем в нем делается запись» [4. С. 200].

Следует отметить, все доказательства для защиты, которые используют адвокаты в своей практике на электронных носителях – это электронные доказательства. Если же речь идет об оцифрованных данных (использован двоичный код), то в материалах уголовного дела должны отразиться цифровые доказательства. Одновременно с названными вопросами возникает проблема ознакомления с материалами дела, ознакомления с материалами дела иных лиц, обжалования процессуальных решений.

Каждый раз, когда адвокат выстраивает линию защиты, он продумывает какие доказательства ему стоит использовать в качестве основных, они могут быть как письменными, так и устными. У этих доказательств также есть общее родовое понятие – вещественные доказательства [6]. Важно приобщить к материалам дела именно цифровой носитель, на котором есть суть самого информационного ресурса, чтобы им можно было воспользоваться в пользу своего подзащитного.

В Федеральной нотариальной палате, в 2023-м количество запросов на заверение цифровых доказательств выросло на 8% год к году. Услуга фиксирования в интернете оскорблений или мошенничества пользуется особой популярностью у жителей Москвы, Санкт-Петербурга, Краснодарского края и Башкортостана.

С. В. Калитин, считая недопустимым смешение понятий, пишет: «...возникшая... путаница в использовании терминов электронный и цифровой привела не только к их взаимозамещающему употреблению, но и к неправильному литературному переводу... Цифровой сигнал не может деградировать под действием кислорода или солнечного (ультрафиолетового) света как его носитель, например, органическая пластмасса на оптическом диске. Цифровые доказательства не меняются. Меняется состояние носителя» [2].

Заключение. Граждане Российской Федерации по статистике чаще используют интернет-пространство, следовательно, чаще обращаются к электронным ресурсам. Человеку проще совершать действия с использованием современных информационных технологий и именно поэтому сделки, договоры и иные общественные отношения становятся доступнее и быстрее для оформления. Правоприменительная практика остро нуждается в методике защиты по преступлениям, административным правонарушениям, связанным с интернетом. Это и клевета, и дискредитация. Помимо этого, растет и гражданская активность людей в социальных сетях. Нынешние реалии таковы, что для того чтобы подтвердить, что правоотношение имеет место быть, нужно показать именно сообщения из мессенджера, а судьи при этом саму переписку в судебном заседании обзирать не желают, ей недостаточно доверяют. Возникает острая необходи-

мость в правовом закреплении статуса цифровых доказательств и обосновании права защитника их использовать в своей деятельности.

Список литературы

1. Воронин М. И. Особенности оценки электронных (цифровых) доказательств // Актуальные проблемы российского права. 2021. № 8(129). С. 118–128.
2. Калитин С. В. Доказательства электронные и цифровые // Концепт. Научно-методический электронный журнал. 2014. Т. 20. С. 3586–3590. URL: <http://e-koncept.ru/2014/54981.htm>
3. Новицкий В. А., Новицкая Л. Ю. Понятие и виды цифровых доказательств // Ленинградский юридический журнал. 2019. № 1(55). С. 213–220.
4. Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т. 12, № 5. С. 200.
5. Шелегов Ю. В., Шелегов В. Г. К вопросу о классификации электронных (цифровых) доказательств // Криминалистика: вчера, сегодня, завтра. 2019. № 2(10). С. 65.
6. Дмитриева А. А., Пастухов П. С. Концепция электронного доказательства в уголовном судопроизводстве // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 270–295. EDN SGAOKS.

Т. В. Радченко,

кандидат юридических наук, доцент,

МИРЭА – Российский технологический университет

ПРАВОВЫЕ И ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ДЕТЕРМИНАЦИИ ТЕРМИНОЛОГИЧЕСКОГО АППАРАТА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ КВАЛИФИКАЦИИ

Аннотация. В настоящей статье осуществлен сравнительный анализ понятий и терминов, имеющих как уголовно-правовое, так и информационно-технологическое значение соответственно. Предпринята попытка исследования правовой природы понятий «компьютерная информация», «охраняемая законом компьютерная информация», «вредоносное программное обеспечение», закрепленных законодательно и терминов «компьютерный инцидент», «инцидент информационной безопасности», используемых в сфере информационных технологий в связи с взаимопроникновением терминологического аппарата и возникающими в этой связи проблемами уголовно-правовой квалификации деяний. Сформулирован тезис о необходимости нормативного закрепления дефиниций «вредоносное программное обеспечение», «компьютерный инцидент» во избежание квалификационных ошибок и повышения эффективности борьбы с киберпреступлениями.

Ключевые слова: компьютерная информация, охраняемая законом компьютерная информация, вредоносное программное обеспечение, компьютерный

инцидент, инцидент информационной безопасности, уголовная ответственность, правила квалификации

LEGAL AND INFORMATION TECHNOLOGICAL ASPECTS OF DETERMINING THE TERMINOLOGICAL APPARATUS OF CRIMES IN THE SPHERE OF COMPUTER INFORMATION: PROBLEMS OF CRIMINAL LAW QUALIFICATION

Abstract. This article provides a comparative analysis of concepts and terms that have both criminal-legal and information-technological significance, respectively. An attempt has been made to study the legal nature of the concepts of "computer information", "legally protected computer information", "malicious software" enshrined in law and the terms "computer incident", "information security incident" used in the field of information technology in connection with the interpenetration of the terminology and the problems of criminal-legal qualification of acts arising in this regard. A thesis has been formulated on the need for normative consolidation of the definitions of "malicious software", "computer incident" in order to avoid qualification errors and improve the effectiveness of the fight against cybercrime.

Keywords: computer information, computer information protected by law, malware, computer incident, information security incident, criminal liability, qualification rules

Введение. Современные темпы цифровизации всех сфер и процессов производственной и социальной деятельности определяют не только прогрессивные тенденции развития общества, но и имеют негативную сторону: рост числа так называемых киберпреступлений – деяний, совершаемых с использованием компьютерной техники, информационно-телекоммуникационных технологий, в сети Интернет. Статистика свидетельствует, что удельный вес данных преступлений составляет 1/3 от числа всех зарегистрированных преступлений за 2023 год, демонстрируя тенденцию к росту на 29,7 % к показателям 2022 г. [5]. В связи с этим особое значение и важность приобретает разработка эффективного механизма уголовно-правового воздействия на подобные негативные действия. Соответствующие нормы уголовного закона позволяют не всегда точно и однозначно квалифицировать совершенное деяние.

Основная часть. Перечень преступлений в IT сфере/киберпреступлений является достаточно обширным, включая не только преступления, закрепленные в гл. 28 УК РФ, но и все деяния, содержащие в качестве квалифицирующего признака «использование ИКТС, в том числе сети Интернет». Однако в рамках заявленной проблемы, полагаю целесообразным осветить проблемы уголовно-правовой характеристики признаков преступлений в сфере компьютерной информации, поскольку правоприменительная практика в отношении указанных норм неединообразна и постановление Пленума ВС РФ от 15.12.2022 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» не проясняет многие вопросы, несмотря на ожидания правоприменителя.

Возможно выделить по меньшей мере 2 группы проблем, возникающих при квалификации данных преступлений:

- 1) связанные с точным определением терминов;
- 2) определяющие применимые правила квалификации.

Итак, понятия, анализируемые в рамках настоящей статьи, закрепленные в УК РФ, определены частично и нечетко. Нормы уголовного закона в этой части бланкетные, а в отраслевом законодательстве термины также не имеют исчерпывающих дефиниций. Это и приводит к необоснованно расширительному толкованию уголовного закона. Такие понятия как «компьютерная информация», «охраняемая законом компьютерная информация» и «критическая информационная инфраструктура РФ», выступая специфическими предметами преступных посягательств, толкуются правоприменителем не единообразно.

В частности, «компьютерная информация» и «охраняемая законом компьютерная информация» имеют совершенно разные характеристики: в первом случае дано законодательное определение, но оно, по сути, неприменимо для характеристики понятия, употребляемого в диспозиции статьи – «охраняемая законом компьютерная информация, когда для признания таковой необходимо установления 2-х условий: нормативного – законом закреплен специальный режим правовой защиты, ограничен доступ и т.д. и охранительного – обладателем информации определены средства защиты, направленные на обеспечение ее целостности и (или) доступности) [7. С. 205.]. Таким образом, правоприменитель определяет информацию как охраняемую при установлении правообладателем даже минимальной ее защиты в виде создания пароля при входе в файловую систему. Представляется, что такое толкование представляется излишне расширительным, ввиду субъективности оценки степени общественной опасности в каждом случае совершенного доступа. Здесь требуется ответ на вопрос: всегда ли содержащаяся в компьютерном устройстве информация настолько значима, что действия с ней общественно опасны. Между тем, вопрос не разрешен однозначно до настоящего момента.

Анализ признаков понятия «вредоносная компьютерная программа или вредоносное программное обеспечение», выступающие предметом преступного посягательства согласно ст. 273 УК РФ затруднены из-за сложности определения технических признаков вредоносности. По признанному мнению, вредоносными являются программы, направленные на осуществление несанкционированного доступа. В связи с этим исследование соотношения понятий «программное обеспечение» и «вредоносное программное обеспечение» позволит избежать ошибок при уголовно-правовой квалификации деяний, посягающих на компьютерную информацию. В этой связи следует охарактеризовать и сопоставить понятия «компьютер» и «компьютерная информация», выявив их существенные признаки. Так, под компьютером понимают «устройство, которое выполняет логические операции и обработку данных, может использовать устройства ввода и вывода информации на дисплей и обычно включает в себя центральный процессор (от англ. CPU – “central processing unit”) для выполнения операций», согласно Техническому регламенту Евразийского экономического союза «О требованиях к энергетической эффективности энергопотребляющих устройств»[4], тогда как под «компьютерной информацией» понимаются сведения (сообщения,

данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Для штатной работы компьютера, т.е. для осуществления любых действий с компьютерной информацией необходимы установка и использование программного обеспечения. С позиции международных стандартов определения понятия «программное обеспечение» (далее – ПО) сводятся к следующему:

- совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ [2];
- все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993) [12];
- компьютерные программы, процедуры и, возможно, соответствующая документация и данные, относящиеся к функционированию компьютерной системы [11].

Действующее Гражданское законодательство РФ, определяя компьютерную программу, использует в ст. 1261 понятие «программа для ЭВМ», закрепляет ее как «...представленную в объективной форме совокупность данных и команд, предназначенную для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения».

Используя метод синтеза, можно сделать вывод о том, что программное обеспечение – особый вид компьютерной информации, содержащий данные и инструкции, позволяющий компьютеру выполнить определенные действия в рамках алгоритма. При этом его программное обеспечение (далее – ПО) может быть использовано в разных целях, в том числе и для нанесения вреда. И тогда оно приобретает свойства вредоносности.

В соответствии с техническими характеристиками существует большое количество определений вредоносного ПО. Так, по глоссарию «VMWare» «Вредоносное ПО – это общее название категории ПО, используемого в киберпреступлениях, которые затрагивают ноутбуки, настольные компьютеры, серверы, мобильные устройства, а в последнее время и устройства Интернета вещей» [1]. Компания «Microsoft» определяет ВПО как «вредоносные приложения и код, способные вызвать повреждения и нарушить нормальную работу устройств. Вредоносные программы позволяют свободно использовать системные ресурсы, запускают несанкционированный доступ, снимают защиту и способствуют краже паролей, блокируют доступ к компьютеру, и выполняют другие действия» [13].

Исходя из вышесказанного, представляется, что вредоносное программное обеспечение – это особый вид компьютерной информации, содержащий данные и инструкции, наносящей вред компьютеру. Следует отметить, однако, что и легитимное ПО может причинить вред. Иными словами, его легко трансформировать во вредоносное.

Уголовный закон РФ не использует указание на какие-либо специальные свойства, обобщая понятие «вредоносное программное обеспечение» (далее – ВПО) до указания на «заведомо предназначенные для несанкционированного

уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты компьютерной информации.

Представляется, что с целью разграничения полезного ПО и вредоносного необходимо использовать специфические показатели, которые можно было бы назвать метриками и установление которых позволит избежать ошибок при квалификации киберпреступлений. К ним следует отнести:

- причиненный ущерб;
- отсутствие согласия пользователя;
- умысел;
- свойства и возможности компьютерной программы.

Одной из важнейших среди представленных метрик ВПО полагаем отсутствие согласия пользователя компьютера на установку данного программного обеспечения. Помимо этого, одним из значимых критериев выступают умышленные действия разработчика ПО, заранее придающего ему скрытую вредоносность. Признание подобного подхода позволит разграничить программную ошибку, нарушение правил использования ПО, повлекшее ущерб и собственно использование ВПО.

Кроме того, размер причиненного ущерба может быть разным: от неисчисляемого морального (программы-шутки) до имущественного вреда в несколько миллионов и более рублей (шифровальщики) [8]. Наконец, стоит отметить, что немаловажную часть в этих метриках играют возможности и информационно-технические способности программы. Программа без функций доступа к файловой системе и сети неспособна нанести какой-либо значительный ущерб.

Таким образом, представляется, что использование обозначенных характеристик/метрик для анализа ПО на вредоносность вполне оправдано и полезно, поскольку позволяет избежать ошибок при разграничении смежных составов преступлений, предусмотренных статьями 272, 273, 274 УК РФ.

Кроме того, бланкетность исследуемых уголовно-правовых норм отсылает правоприменителя, как правило, к отраслевым актам – национальным стандартам – ГОСТам, оперирующим отличными от уголовного закона понятиями «инцидент», «инцидент информационной безопасности» и «компьютерный инцидент/киберинцидент», которые в свою очередь указывают и характеризуют способ и результат воздействия на информационную инфраструктуру. При этом данные понятия не синонимичны.

Так, анализ функционирования ИТ-систем в бизнес-сфере позволяет констатировать, что указанные понятия имеют существенные различия, а также определяют разные ситуации.

Под «инцидентом» обычно понимают спонтанные снижение качества или прерывание предоставления ИТ-услуг или реализации бизнес-процессов. Это может быть квалифицировано как деликт или казус, разграничивая невиновное причинение вреда с обстоятельствами непреодолимой силы – как чрезвычайное и непредотвратимое при данных условиях обстоятельство.

Причиной таковых, как правило, являются различные технологические факторы, например, устаревшее оборудование, уязвимые личные устройства сотрудников; человеческий фактор, не связанный с умыслом на причинение вреда. По уровням объема и охвата операций такие инциденты типизируют как низкий,

средний, высокий, критический. Данное деление используется с целью определения приоритетности устранения ввиду влияния инцидента на бизнес и прогнозируемые затраты на восстановление.

«Инцидент ИБ» – одно или несколько событий, с высокой вероятностью приводящих к угрозе информационной безопасности и функционирования бизнес-процессов. Согласно ГОСТ Р ИСО/МЭК ТО 18044-2007 ФСТЭК России «Менеджмент инцидентов информационной безопасности» под «инцидентом ИБ» понимают появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана незначительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности. В данной характеристике использованы оценочные признаки, сами по себе нуждающиеся в четком определении: нежелательные, неожиданные, спонтанные... [3]. Толкование подобных признаков обычно затруднено.

В свою очередь, «Событие ИБ» – зафиксированное состояние информационной (автоматизированной) системы, указывающее на возможное нарушение безопасности информации, сбой средств защиты информации или ситуацию, которая может быть значимой для безопасности информации.

Под компьютерным инцидентом (киберинцидентом) [6] понимают факт нарушения и/или прекращения функционирования информационного ресурса, сети электросвязи, используемых для организации взаимодействия информационных ресурсов, и/или нарушения безопасности обрабатываемой информации, в т.ч. произошедший в результате компьютерной атаки.

В этом случае возможно установить общественную опасность или как минимум вредность. По этой причине важна оценка ситуации с точки зрения закона, императивно предусматривающего юридическую ответственность.

Однако ни материальное, ни процессуальное действующее законодательство РФ не знают понятий «инцидент», «инцидент ИБ», «киберинцидент» при установлении оснований конкретного вида ответственности, например, при неправомерном доступе к компьютерной информации, или посягательстве на персональные данные.

Безусловно посредством толкования правоприменитель придет к выводу что инцидент – это событие, которое произошло при совершении кибератаки (конкретного типа), который в свою очередь будет отвечать признакам способа совершения деяния.

В сфере информационной безопасности названы несколько типов компьютерных инцидентов, подпадающих либо под характеристику признаков объективной стороны ст. 273 УК РФ – использование вредоносного ПО (заражение), либо направленных на копирование, блокирование, модификацию, уничтожение информации по смыслу 272 УК РФ (DoS-атаки, несанкционированный доступ, стороннее сканирование и т.д.). При этом уголовный закон предусматривает усеченную ответственность за посягательства на компьютерную информацию, тогда как понятие кибербезопасность охватывает еще и безопасность работы устройств, оборудования и ПО.

Следует отметить, что понятие «киберинцидент» до сих пор остается отчасти оценочным, поскольку закреплено на уровне отраслевого регулирования. Как правило, специалисты в сфере информационной безопасности считают его либо пра-

вонарушением особого рода с возможностью привлечения нарушителя к дисциплинарной ответственности, либо не влекущим юридической ответственности событием. Более того, не всегда устранение последствий кибервоздействия ведет к установлению лица, его совершившего. Более того, инциденты часто транграничны. Таким образом, проблема понимания правовой природы вышеуказанных понятий порождает проблемы уголовно-правовой квалификации деяний.

Применимые правила квалификации анализируемых деяний также нуждаются в уточнении. Зачастую, при неправомерном доступе к компьютерной информации, особенно удаленном, используется вирусное программное обеспечение как способ неправомерного доступа [9. С. 131]. В этом случае, по мнению Верховного Суда РФ, следует квалифицировать действия виновного по совокупности преступлений ст. 272 и 273 УК РФ. Более того, в случае посягательства на охраняемую законом тайну, например, частной жизни, также по ст. 138 УК РФ, тогда как при использовании вредоносных компьютерных программ для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (в том числе в случае, когда осуществляется распространение этих программ на объекты критической информационной инфраструктуры исключительно для их последующего использования) полностью охватывается ч. 2 ст. 274¹ УК РФ и дополнительной квалификации по ст. 273 УК РФ не требует [10. С. 53].

Резюмируя изложенное, следует особо отметить, что обозначенные ситуации не способствуют единообразному применению уголовного закона и требуют его доработки. Представляется, что этот процесс должен быть как безусловно качественным с точки зрения правового анализа, применимой юридической техники, так и максимально интенсивным в силу стремительного развития ИТ-технологий.

Заключение. Повседневная деятельность человека с неизбежностью предполагает взаимодействие с устройствами и технологиями, которые стремительно меняют представление о реальности [14. С. 652]. Преступная деятельность в ИТ-сфере высокоинтеллектуальна и, соответственно, латентна, способы ухода от ответственности постоянно совершенствуются, поэтому алгоритмы правового реагирования должны соответствовать этим вызовам. Однако их создание и эффективное использование возможно лишь при глубоком понимании сути процесса: при активном диалоге не только юристов, но и ИТ-специалистов.

Список литературы

1. Глоссарий VMWare: Вредоносное ПО. 2024. URL: <https://www.vmware.com/ru/topics/glossary/content/malware.html> (дата обращения: 26.04.2024).
2. ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения // Единая система программной документации: Сб. ГОСТов. М.: Стандартинформ, 2010.
3. ГОСТ Р ИСО/МЭК ТО 18044-2007 ФСТЭК России «Менеджмент инцидентов информационной безопасности» режим. URL: <https://base.garant.ru/70246074> (дата обращения: 02.09.2024).

4. Евразийский экономический союз. Официальный сайт. 2024. URL: <http://www.eaeunion.org> (дата обращения: 16.08.2024).
5. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года [Электронный ресурс]. URL: <https://мвд.рф/reports/item/47055751/?ysclid=m0oaq7qak6659947758> (дата обращения: 02.09.2024).
6. Национальный стандарт РФ ГОСТ 59709 – 2022 Защита информации. Управление компьютерными инцидентами. Термины и определения. Утв. Приказом Федерального агентства по техническому регулированию и метрологии. URL: <https://base.garant.ru/406006283> (дата обращения: 02.09.2024).
7. Пучков Д. В. Объективные признаки преступлений по законодательству РФ, совершаемых в сфере реализации кибернетических технологий // Гуманитарные и юридические исследования. 2019. № 4.
8. Рафиков И. Н., Алышев Ю. В. Преступления в сфере компьютерной информации // E-Scio. 2020. № 2 (41).
9. Теппеев А. А. Способы совершения и проблемы квалификации преступлений, совершаемых с использованием сети интернет // Право и управление. 2023. № 3.
10. Шульга А В., Галиакбаров Р. Р. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) // Гуманитарные, социально-экономические и общественные науки. 2018. № 5.
11. IEEE Standard for Software and System Test Documentation // IEEE Std 829-2008. 2008. Pp. 1–150. (дата обращения: 18.02.2023).
12. ISO/IEC 2382:2015 Information technology – Vocabulary. 29.11.2022. URL: <https://www.iso.org/standard/63598.html> (дата обращения: 18.02.2023).
13. Understanding malware & other threats. 29.11.2023. URL: <https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/understanding-malware> (дата обращения: 20.01.2024).
14. Русскевич Е.А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650–672. <https://doi.org/10.21202/jdtl.2023.28>. EDN: fiseet

А. Ф. Реховский,

кандидат юридический наук, доцент,
Дальневосточный федеральный университет

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В УГОЛОВНОМ ПРАВОСУДИИ: АНАЛИЗ ОГРАНИЧЕНИЙ И ЭТИЧЕСКИХ ВЫЗОВОВ В СВЕТЕ ЕВРОПЕЙСКОГО ЗАКОНА ОБ ИСКУССТВЕННОМ ИНТЕЛЛЕКТЕ

Аннотация. В статье исследуется влияние цифровизации на уголовную юстицию, с акцентом на использование искусственного интеллекта (ИИ). Цель работы заключается в анализе ограничений и этических вызовов, связанных с внедрением ИИ, в свете принятия Европейского закона об искусственном ин-

теллекте от 2024 года. Рассматриваются ключевые положения закона, включая категоризацию ИИ-систем по уровням риска и ограничения на их использование в сфере уголовного правосудия. Особое внимание уделено вопросам прогнозирования преступного поведения, биометрической идентификации, а также соблюдению прав человека и этических стандартов.

Ключевые слова: искусственный интеллект, уголовное правосудие, Европейский регламент об ИИ, этические вызовы, правовое регулирование

ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE: ANALYSIS OF LIMITATIONS AND ETHICAL CHALLENGES IN THE CONTEXT OF THE EUROPEAN ARTIFICIAL INTELLIGENCE ACT

Abstract. The article examines the impact of digitalization on criminal justice, with a focus on the use of artificial intelligence (AI). The objective of the study is to analyze the limitations and ethical challenges related to the implementation of AI in light of the adoption of the European Artificial Intelligence Act of 2024. The key provisions of the law are reviewed, including the categorization of AI systems based on risk levels and the restrictions on their use in criminal justice. Special attention is given to issues such as crime prediction, biometric identification, and the protection of human rights and ethical standards.

Keywords: artificial intelligence, criminal justice, European AI regulation, ethical challenges, legal regulation

Введение. Цифровизация правосудия и внедрение передовых технологий, таких как искусственный интеллект (ИИ), становятся неотъемлемой частью модернизации судебных систем во всем мире. Особое значение этот процесс приобретает в контексте уголовного правосудия, где возможности ИИ могут существенно повлиять на правоприменение, принятие решений и соблюдение прав граждан. В уголовном процессе возможности применения ИИ безграничны: возможно применение технологий в целях профилактики и выявления преступлений, организация предварительного расследования, криминалистическое сопровождение расследования преступлений, оценка доказательств на досудебной и судебной стадиях [7. С. 490]. Тем не менее широкое использование ИИ в данной сфере связано с рядом этических и правовых вызовов, включая вопросы прозрачности, дискриминации и защиты прав человека. В свете принятия Европейского закона об искусственном интеллекте 2024 года особенно остро встает необходимость анализа ограничений и рисков, связанных с применением ИИ в уголовной юстиции. Настоящая статья посвящена рассмотрению ключевых положений этого закона, влиянию его на судебные практики и этическим аспектам, связанным с внедрением ИИ в правоохранительные органы.

Основная часть. С методологической точки зрения справедливо отмечено, что «... особые трудности проектировщики цифровизации уголовного судопроизводства испытывают в связи с тем, что сегодня ни в области теоретической физики, ни в области социальных и гуманитарных наук нет единых господствующих теорий – каждая отрасль знания представлена множеством теорий и концепций, а в использовании теоретического знания растут рефлексивно-

методологическая и критико-рефлексивная составляющие» [1. С. 6]. Сходную мысль высказал и Ядун Цуй «Не существует готового пути для реформирования и инноваций судебной системы Китая» [4. С. 11].

Европейский Союз продемонстрировал прогрессивный подход к регулированию цифровизации в сфере уголовной юстиции, что наглядно иллюстрируется принятием Регламента об искусственном интеллекте (далее – «Регламент») от 13 марта 2024 года [3]. Данный нормативный акт представляет собой первую в мире комплексную правовую базу, регулиующую использование ИИ во всех сферах, включая уголовное правосудие.

Основная цель Регламента заключается в обеспечении этичного и безопасного использования ИИ с минимизацией рисков для прав человека и фундаментальных свобод. Документ вводит категоризацию систем ИИ по уровням риска (низкий, средний, высокий и неприемлемый) и устанавливает соответствующие требования к их применению.

В контексте уголовной юстиции Регламент предусматривает строгие требования и ограничения для систем ИИ, используемых в предсказательной аналитике преступлений, распознавании лиц и биометрической идентификации. Для высокорисковых ИИ-систем предписывается проведение обязательных оценок риска, обеспечение прозрачности алгоритмов, защита данных и независимый аудит.

Особое внимание в Регламенте уделяется запретам и ограничениям на использование определенных типов ИИ в уголовной юстиции. В частности, вводятся строгие ограничения на применение «социального скоринга» и дистанционного биометрического распознавания в реальном времени в общественных местах, за исключением четко определенных чрезвычайных ситуаций, таких как угроза терроризма.

Таким образом, Регламент об искусственном интеллекте демонстрирует комплексный подход Европейского Союза к регулированию ИИ, направленный на достижение баланса между инновационным развитием и защитой фундаментальных прав граждан, а также на обеспечение использования ИИ в уголовной юстиции в строгом соответствии с высокими стандартами безопасности, этики и прозрачности.

Более глубокий анализ данного нормативного акта позволяет выделить несколько ключевых аспектов, представляющих значительный интерес для исследования.

Во-первых, важным является определение понятия «системы искусственного интеллекта». Согласно пункту 12 Регламента, система искусственного интеллекта определяется как машинная система, отличительной характеристикой которой является способность делать умозаключения. Эта способность позволяет системе генерировать результаты в виде прогнозов, содержания, рекомендаций или решений, оказывающих влияние на физическую или виртуальную среду, а также создавать модели и алгоритмы на основе исходных данных. Такие системы применяют методы, выходящие за пределы стандартной обработки данных, включая машинное обучение и подходы, основанные на логике и знаниях. Они могут функционировать с различными уровнями автономности и адаптивности, действуя как автономно, так и в составе других изделий.

Во-вторых, требования к искусственному интеллекту, разработанные Европейской комиссией как основа для разработки, внедрения и эксплуатации надежных и этически обоснованных ИИ-систем, включая их применение в сфере уголовного правосудия, можно свести к следующим критериям:

1. Превосходство человека и надзор: ИИ-системы обязаны поддерживать автономию человека, предоставлять возможности для вмешательства и контроля со стороны людей, а также соблюдать основные права личности.

2. Техническая надежность и безопасность: ИИ-системы должны гарантировать безопасность пользователей, быть защищенными от внешних угроз и включать механизмы защиты, способные срабатывать в непредвиденных ситуациях.

3. Разнообразие, недискриминация и справедливость: разработка ИИ-систем должна учитывать принципы равенства и недопущения дискриминации, гарантируя справедливое отношение ко всем социальным группам.

4. Прозрачность: системы ИИ должны быть максимально прозрачными, предусматривая наличие полной документации на всех этапах – от сбора данных до процессов разработки, чтобы обеспечить аудит и понимание их функционирования.

5. Конфиденциальность и управление данными: ИИ-системы обязаны уважать право на конфиденциальность, обеспечивая надежную защиту персональных данных, с доступом исключительно для уполномоченных лиц.

6. Социальное и экологическое благополучие: ИИ-системы должны содействовать улучшению общественного благосостояния и экологической безопасности, исключая негативное воздействие на окружающую среду и общество [5].

Эти критерии отражают стремление Европейской комиссии к обеспечению баланса между технологическим прогрессом и защитой прав человека, что особенно важно при внедрении ИИ в такие чувствительные сферы, как уголовное правосудие.

В-третьих, Регламент относит ИИ-системы, применяемые в уголовной юстиции стран Европейского Союза, к категории высокорисковых систем. В эту категорию входят системы, предназначенные для использования правоохранительными органами, а также связанные с управлением миграцией, предоставлением убежища и пограничным контролем. Кроме того, к высокорисковым относятся ИИ-системы, применяемые в отправлении правосудия и поддержке демократических процессов, включая системы, которые используются судебными органами или по их поручению для анализа и интерпретации фактов и норм права, а также при принятии правовых решений в отношении конкретных дел [2]. Эти системы также могут применяться для альтернативных методов разрешения споров.

Таким образом, высокая степень риска обусловлена прямым воздействием ИИ-систем на фундаментальные права человека, правоприменительную практику и процесс принятия решений, что требует строгого регулирования и контроля их использования.

В-четвертых, Регламент устанавливает запрет на использование предсказательной аналитики в деятельности полиции, в том числе для прогнозирования вероятности рецидивов преступлений. Это положение ограничивает возможности предиктивных технологий и может оказать негативное влияние на развитие таких инновационных дисциплин, как киберкриминология и кибервиктимология.

В пункте 42 Регламента подчеркивается: «В соответствии с принципом презумпции невиновности лица в Европейском Союзе должны оцениваться исключительно на основе их фактического поведения. Оценка людей не может основываться на прогнозах, полученных с использованием ИИ, если они опираются только на профилирование, личные характеристики или черты характера». Таким образом, проведение оценки риска совершения преступлений или прогнозирования криминальных действий, опираясь исключительно на профилирование или анализ личностных черт, категорически запрещается.

Это положение отражает стремление Европейского союза к защите прав и свобод граждан, исключая возможность предвзятого отношения к физическим лицам на основе автоматизированных прогнозов, что ограничивает использование ИИ в данной сфере и требует пересмотра методов работы с преступными рисками.

Мы солидарны с мнением современных исследователей о том, что предложенный Европейской Комиссией «Закон об ИИ», который стремится регулировать использование ИИ во всех системах уголовного правосудия ЕС, а также аналогичные инициативы в Совете Европы, обещают стать важным шагом вперед, хотя многие аспекты его содержания еще требуют дальнейшего обсуждения [6. С. 68].

Европейский закон об искусственном интеллекте 2024 года представляет собой амбициозную попытку установить стандарты для применения ИИ в различных сферах, включая уголовное правосудие.

Европейский Регламент об искусственном интеллекте вводит строгие ограничения на использование ИИ в уголовном правосудии, фактически исключая его широкое применение для прогнозирования преступного поведения и рецидива в странах Европейского Союза. Регламент делает акцент на защите фундаментальных прав человека и предотвращении дискриминации, что предполагает минимизацию рисков, связанных с внедрением ИИ в судебные процессы, а также требует соблюдения строгих стандартов этики и правовых норм.

Эти ограничения отражают необходимость учета этических и правовых аспектов использования ИИ, что, с одной стороны, снижает риски дискриминации и несправедливости, а с другой – создает вызовы для технологических инноваций в области правосудия. Закон может оказывать значительное влияние на глобальные подходы к регулированию ИИ, способствуя международной гармонизации стандартов и развитию более ответственного использования ИИ.

Будущие исследования и эмпирические данные о применении Европейского закона об ИИ позволят более точно оценить его влияние на судебную систему, выявить возможные улучшения и определить направления для дальнейшего развития законодательства.

Заключение. Европейский закон об искусственном интеллекте представляет собой важный шаг на пути к созданию ответственного и безопасного использования ИИ в различных сферах, включая уголовное правосудие. Введение строгих стандартов для ИИ-систем направлено на защиту фундаментальных прав человека, предотвращение дискриминации и обеспечение прозрачности алгоритмов. Тем не менее, внедрение таких ограничений также создает определенные вызовы для дальнейшего развития технологий, в частности, в области пред-

сказательной аналитики и криминологии. Будущее использование ИИ в правосудии будет требовать тщательного баланса между инновационными возможностями и необходимостью соблюдения этических норм и стандартов прав человека, что в итоге будет способствовать более справедливому и прозрачному правоприменению.

Список литературы

1. Воскобитова Л. А. Уголовное судопроизводство: трансформация теоретических представлений и регулирования в условиях цифровизации: монография / отв. ред. Л. А. Воскобитова, В. И. Пржиленский. – Москва: НОРМА: ИНФРА-М, 2022. – 288 с. – DOI 10.12737/1893198. Текст : электронный. URL: <https://znanium.ru/catalog/product/1893198> (дата обращения: 21.08.2024).
2. Регламент Европейского союза об искусственном интеллекте. Анализ основных положений и принципов регулирования. АНО «Цифровая экономика», 2024. URL: https://ai.gov.ru/knowledgebase/dokumenty-po-razvitiyu-ii-v-drugikh-stranakh/2024_reglament_evropeyskogo_soyuza_ob_iskusstvennom_intellekte_ano_cifrovaya_ekonomika/
3. Artificial Intelligence Act European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). – URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-03-3_EN.html#sdocta2.
4. Cui, Yadong. Artificial Intelligence and Judicial Modernization. Singapore: Springer Singapore, 2020. <https://doi.org/10.1007/978-981-32-9880-4>.
5. Farayola, Michael Mayowa, Irina Tal, Regina Connolly, Takfarinas Saber, and Malika Bendeche. «Ethics and Trustworthiness of AI for Predicting the Risk of Recidivism: A Systematic Literature Review». Information 14, вып. 8 (27 июль 2023 г.): 426. <https://doi.org/10.3390/info14080426>
6. Sprenger, J. M., Brodowski, D. Predictive policing, predictive justice, and the use of artificial intelligence in the administration of criminal justice in Germany // Journal of Legal Studies. – 2023. – № 5. – С. 45–68.
7. Spiridonov M. S. Artificial Intelligence Technologies in Criminal Procedural Proving // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481–497. <https://doi.org/10.21202/jdtl.2023.20>. EDN: acsqxh

В. И. Романов,
кандидат юридических наук, доцент,
Казанский (Приволжский) федеральный университет

К ВОПРОСУ О ЦИФРОВИЗАЦИИ В РАБОТЕ СЛЕДОВАТЕЛЯ

Аннотация. Настоящая статья посвящена работе следователей в условиях цифровизации. Вопросы цифровизации представляют собой актуальность, востребованность и интерес в изучении, в том числе и в уголовно-правовой среде. Средства цифровизации помогают оптимизировать процесс расследования, эффективно решать проблемы, связанные с поиском доказательств по уголовному делу.

Ключевые слова: цифровизация, информационные технологии, следственные органы, преступление, информация, доказательство

ON THE ISSUE OF DIGITALIZATION IN THE WORK OF AN INVESTIGATOR

Abstract. This article is devoted to the work of investigators in the context of digitalization. The issues of digitalization are relevant and interesting to study, including in the criminal law environment. Digitalization tools help to optimize the investigation process and effectively solve problems related to the search for evidence in a criminal case.

Keywords: digitalization, information technology, investigative agencies, crime, information, evidence

В современном мире о цифровых возможностях свидетельствуют новые инструменты криминалистической техники и тактики. Многие вопросы на теоретическом и практическом уровнях вызывают интерес.

Средства цифровизации оказывают влияние на развитие криминалистики, положительно влияя на процесс расследования многих современных преступлений.

Цифровизация приводит к образованию особых следов, так называемых «цифровых следов». Работа с цифровыми следами обладает особой спецификой, следователь успешно решает следующие задачи:

- использование современных криминалистических средств, способных выявлению следов преступной деятельности лица;
- формирование данных спутниковых систем;
- применение программного обеспечения (например, программ Cell Catcher, NetMonitor, Entropy и др.);
- понятие аналитических действий в составе оперативности нахождения информации;
- использование автомобильных регистраторов и видеокамер при осмотре помещений, местности и последующем их использовании в уголовном процессе.

Информационно-телекоммуникативные цифровые возможности улучшают и во многом облегчают жизнь современного человека, что, несомненно, является положительным аспектом. Однако наряду с этим, мы не можем не наблюдать и отрицательные аспекты увеличения преступности с использованием цифровой среды.

Увеличение количества преступлений с использованием новейших цифровых систем требует от правоохранительных органов профессионализма, сосредоточенности, знаний. Следователи постоянно совершенствуют свои возможности по работе с цифровыми следами как носителями информации о совершенном преступлении. На наш взгляд, наиболее приемлемыми способами обнаружения цифрового следа являются:

- определение специфики проявления следа в результате совершенного преступления;
- обнаружение следа с учетом географических свойств и географии его распространения.

Преступники стараются с каждым годом совершенствовать свое мастерство, стараются усовершенствовать способы осуществления незаконной деятельности в целях уменьшения вероятности их раскрытия и привлечения к уголовной ответственности. Например, активно используются возможности скрытого сегмента интернета – DarkNet, свидетельствующие о повышенной степени анонимности, способности скрыть информацию о владельце, посещающем тот или иной сайт в интернет-пространстве.

Цифровые следы присутствия могут быть оставлены на мобильных устройствах, планшетах, ноутбуках и иной технике, активно применяемой в повседневной жизни. Обнаружение таких следов позволяет определить время нахождения преступника на сайте в системе интернет, оценить его действия, цели и желания [3. С. 120].

Фиксация цифровых следов осуществляется следователем или дознавателем при помощи изъятия устройства, копирования или переноса информации на магнитный носитель. Изъятая информация подлежит тщательному осмотру, изучению. В настоящее время проблема состоит в том, что информация может сохраняться одновременно на нескольких серверах, местах, находящихся далеко от места производства предварительного следствия. В частности, на территории соседнего субъекта или даже иного государства.

В качестве примера. При расследовании уголовного дела, возбужденного по ч. 1 ст. 30 и ч. 1 ст. 223.1 УК РФ наряду с привычными доказательствами были изучены протоколы осмотра оптических дисков, содержащих результаты оперативно-разыскной информации, полученные в результате снятия информации с технических каналов связи [6].

Однако не всегда и не во всех случаях цифровые следы могут положительно сказываться на результатах расследования. Так, в результате судебного разбирательства довод, изложенный в апелляционной жалобе о том, что специалист не принимал участие в изъятии жесткого диска при проведении обыска, осмотра цифровой информации с технического устройства – ноутбук, не было принято во внимание. Судом было установлено, что процесс изъятия информации путем копирования технически не осуществлялся [7].

Современные мобильные устройства, помимо сигналов и приложений (мобильного банкинга), графических, текстовых, аудио- и видеосообщений в мессенджерах и социальных сетях фиксируют четко информацию о пользователе. В результате изучения технического и программного устройства человека можно обнаружить: места его пребывания; покупательскую способность

и предпочтения; круг интересов, общения; социальную предрасположенность к окружающему мнению и многие другие сведения.

Следователь, изучая мобильник подозреваемого может узнать много новой информации о его владельце, особенно в части сведений, интересующих следствие и о которых скрывает, молчит задержанный [5. С. 44].

Развитие криминалистики в рамках технических разработок позволяет качественно и профессионально обеспечивать изучение таких устройств, добывать информацию, в последующем ее использовать. Отметим то, что цифровизация в работе следственных органов позволяет улучшить специфику процесса раскрытия и расследования многих преступлений. Судебно-следственная практика позволяет не только находить, выявлять цифровые следы, но и работать с ними при помощи аппаратно-программных комплексов.

Список литературы

1. Конституция РФ – М.: Проспект, 2022.
2. Уголовно-процессуальный кодекс РФ (с изменениями и дополнений на 2023 г.). – М.: Проспект, 2023.
3. Лавров В. П., Шалимов А. Н., Романов В. И. и др. Криминалистика. Конспект лекций. – М.: Проспект., 2020. С. 125.
4. Муратова Н. Г., Сергеев М. С. Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: общественный и зарубежный опыт: монография. Юрлитинформ. – М., 2019. С. 44.
5. Романова Г. В. Цифровые доказательства: понятие, особенности, проблемы использования в современном законодательстве и практике его применения: учебное пособие. – Казань: РИЦ «Школа», 2023. – 171 с.
6. Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 05.09.2019 № 201-АПУ19-37.
7. Апелляционное постановление Приморского краевого суда от 24.09.2015 № 22К-5674/2015.

Р. В. Колесников,
кандидат юридических наук,
Воронежский институт МВД России,
В. В. Сенцов,
слушатель,
Воронежский институт МВД России

РОЛЬ «КРИПТОВАЛЮТЫ» В УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЯХ

Аннотация. Внедрение в повседневную жизнь информационных технологий, обуславливает развитие и становление новых общественных отношений, которые необходимо урегулировать законодателю. В свою очередь, происходит значительный рост преступлений, совершенных с использованием информационно-телекоммуникационных технологий, отдельное место отведено совершению преступлений с помощью «криптовалюты». В статье представлены стати-

стические показатели, рассмотрены мнения авторов, а также приведены материалы судебной практики, свидетельствующие об отнесении «криптовалюты» к уголовно-правовым категориям, что является первоочередной целью исследования.

Ключевые слова: цифровые технологии, право, криптовалюта, биткоин, информационно-телекоммуникационные технологии, цифровая валюта, предмет совершения преступления, средство совершения преступления

THE ROLE OF "CRYPTOCURRENCY" IN CRIMINAL LAW RELATIONS

Abstract. The introduction of information technologies into everyday life determines the development and formation of new public relations, which must be regulated by the legislator. In turn, there is a significant increase in crimes committed using information and telecommunications technologies, a separate place is reserved for the commission of crimes using "cryptocurrency". The article presents statistical indicators, reviews the opinions of the authors, and provides materials of judicial practice indicating that "cryptocurrency" belongs to criminal law categories, which is the primary purpose of the study.

Keywords: digital technologies, law, cryptocurrency, bitcoin, information and telecommunication technologies, digital currency, the subject of a crime, a means of committing a crime

Введение. Тема исследования в настоящее время является актуальной, ее практическая необходимость подтверждается стабильным ростом количества зарегистрированных преступлений с активным использованием информационно-телекоммуникационных технологий и средств их совершения. Данные из официальных статистических источников МВД России показывают, что за 2022 г. зарегистрировано – 522 065 фактов преступной деятельности, в свою очередь 2023 г. ознаменован показателем 676 951, тем самым представленные показатели, свидетельствуют об увеличении совершения данной категории преступлений. Пристального внимания заслуживают преступления, совершенные с использованием «криптовалюты», так, по мнению А. Н. Ляско: «Расширение сферы обращения и повышенный криминальный интерес к использованию «криптовалюты» все чаще вынуждают правоприменителя признавать ее предметом или средством преступления» [2. С. 87–92].

Основная часть. К сожалению, российский законодатель до сих пор не определил правовой статус «криптовалюты» и не закрепил его в качестве легального юридического понятия. Хотя в законодательстве есть схожее понятие, закрепленное в ст. 1 Федерального закона РФ от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [2], «цифровая валюта». По нашему мнению и рассуждению ученых-специалистов, термины абсолютно не являются тождественными. Так, М. А. Павлова и Н. В. Бурдакова считают, что «криптовалюта» не является средством расчета, так как формируется децентрализованно без участия и разрешения на то Центрального Банка РФ, и представляет собой лишь виртуальный финансовый актив [3. С. 243–245].

Теоретическое определение термина наиболее точно сформулировал в своей научной работе И. А. Ишин, который отметил, что «криптовалюта» является одним из видов цифровой валюты, формируемой на основе криптографических методов, эмиссия и учет которой осуществляются в децентрализованной форме [4. С. 82–85].

В соответствии с современными цифровыми технологиями в настоящее время существуют следующие виды «криптовалюты», запущенные на основе технологии blockchain: биткоин (самый распространенный), эфириум, лайткоин и др. Необходимо отметить, что данная технология основана на таком принципе работы, который при транзакции можно проследить вплоть до криптографических идентификационных данных, но теоретически они анонимны.

Рассмотрев положение законодательства и мнение некоторых авторов, необходимо определить ряд проблемных вопросов, касаемо роли «криптовалюты» в уголовно-правовых отношениях.

Одним из первых вопросов является: «В случае совершения хищения чужого имущества, может ли «криптовалюта» выступать в качестве предмета совершения преступления?». Как известно, «криптовалюта» хранится на специальных кошельках, которые предназначены для хранения электронных денежных средств и проведения транзакций. Более точное определение «специального кошелька» изложено в научном труде А. А. Коренной, под которым автор понимает программы, на которых хранятся приватные и публичные ключи, а также взаимодействуют с различными «блокчейнами», для отправки и получения цифровой валюты [5. С. 220–223]. В данном случае следует установить принадлежность «криптовалюты» к имуществу. Российское гражданское законодательство не закрепляет «криптовалюту» как объект гражданских прав, что вызывает сложность с установлением в качестве имущества, но научное сообщество сформулировало ряд признаков, на основании которых возможно рассмотреть «криптовалюту» как предмет преступного посягательства, в противоправных деяниях, направленных на хищение чужого имущества. К таковым относят:

- 1) экономический признак (наличие материальной ценности, т. е. оплата товаров и услуг, а также средство инвестирования);
- 2) юридический признак (предполагает нахождение в собственности конкретного лица).

По нашему мнению, «криптовалюта» может выступать в качестве предмета совершения преступления в следующих составах: ст. 158 и ст. 159 УК РФ, так как по своей сути, способ хищения может выглядеть следующим образом: злоумышленник получает устройство тайно или путем обмана, на котором хранится «специальный кошелек», подключает к компьютеру или смартфону и производит транзакцию. Ю. А. Баратов придерживается точки зрения о том, что необходимо одновременно использовать положение Гл. 28 УК РФ, так как хищение «криптовалюты» из специального кошелька, реализуется посредством неправомерного доступа в аккаунт пользователя (собственника «криптовалюты»), тем самым указанные действия посягают на общественные отношения в сфере компьютерной информации [6. С. 148–152].

Немаловажным вопросом является: «Может ли «криптовалюта» выступать в качестве средства совершения преступления?» Рассмотрим примеры судебной

практики, когда с помощью «криптовалюты», происходит покупка наркотических средств. Так, в приговоре Калужского областного суда от 30 января 2024 года, лицо было осуждено по п. а, ч. 4, ст. 174.1 в совокупности с ч. 5 ст. 228.1, ч. 3 ст. 30, ч. 5 ст. 228.1, ч. 3 ст. 30, ч. 5 ст. 228.1 УК РФ. Установлено, что подсудимый вступил в организованную группу, для серийного изготовления и продажи наркотических средств, был разработан план совместных действий и распределены роли. Способ продажи – «тайники». Покупка наркотических средств, осуществлялась с помощью виртуальных активов, представленных в «криптовалюте», на специальные электронные кошельки [7]. Следующим ярким примером, совершения преступлений с помощью виртуальных активов является приговор районного суда г. Зубцова от 25 января 2024 года, лицо было осуждено по ч. 5 ст. 228.1, ч. 2 ст. 238.3 УК РФ. Судом установлено, что осужденный с помощью мессенджера Telegram приобретал за криптовалюту bitcoin наркотические средства, после чего осуществлял сбыт, путем оборудования «тайников» [8].

По нашему мнению, как показывает судебная практика, в действительности возможно воспринимать «криптовалюту» в качестве средства совершения преступления, так как использование данного виртуального актива, возможно для совершения преступления.

Заключение. Таким образом, рассмотрев положение законодательства, мнения авторов [9] и ряд проблемных вопросов, необходимо сформулировать следующие выводы.

Первое, происходит рост IT-преступности, указанные статистические данные позволяют смело говорить об этом. Во-вторых, российское законодательство не закрепляет легального толкования термина «криптовалюта», тем самым вызывает трудности у правоприменителя в квалификации преступлений, совершенных с данным цифровым активом. В-третьих, анализ мнений ученых-теоретиков, специалистов-практиков и материалов опубликованной судебной практики показал важность «криптовалюты» в уголовно-правовых отношениях.

Список литературы

1. Лясколо А. Н. Криптовалюта как предмет и средство преступления // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной конференции. М., 2019. С. 87–92.
2. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон РФ от 31.07.2020 № 259-ФЗ // СПС «КонсультантПлюс», 2024 (дата обращения: 26.08.2024).
3. Павлова М. А., Бурдакова Н. В. Понятие цифрового рубля и его отличия от криптовалют // Юный ученый. 2023. № 3 (66). С. 243–245.
4. Ишин И. А. Особенности производства отдельных следственных действий и роль начальника органа дознания при расследовании преступлений, совершенных с использованием криптовалюты // Академическая мысль. – 2020. – № 2 (11). – С. 82–85.

5. Коренная А. А. Квалификация преступлений, совершаемых с использованием криптовалюты // Проблемы экономики и юридической практики. 2018. № 3. С. 220–223.

6. Баратова Ю. А. Квалификация преступлений, совершаемых с использованием криптовалюты // Право и управление. – 2023. – № 3. – С. 148–152.

7. Приговор Калужского областного суда № 2-2/2024 2-22/2023 УК-2-2/2024 УК-2-22/2023 от 30 января 2024 г. по делу № 2-2/2024 / Суды общей юрисдикции // Судебные и нормативные акты РФ. – URL: <https://sudact.ru> (дата обращения: 26.08.2024).

8. Приговор № 1-13/2024 1-72/2023 от 25 января 2024 г. по делу № 1-13/2024 / Суды общей юрисдикции // Судебные и нормативные акты РФ. – URL: <https://sudact.ru> (дата обращения: 26.08.2024).

9. Ярутин Я. К., Гуляева Е. Е. Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 725–751. <https://doi.org/10.21202/jdtl.2023.32>. EDN: hgbqgl.

Н. А. Силаева,
старший преподаватель,
Казанский инновационный университет
имени В. Г. Тимирязева

ПОЛИЦИЯ КАК СУБЪЕКТ ПРОФИЛАКТИКИ И ЗАЩИТЫ ОТ КРИМИНАЛЬНОЙ ВИКТИМНОСТИ ИНВАЛИДОВ В УСЛОВИЯХ ЦИФРОВОГО ОБЩЕСТВА

Аннотация. В статье рассматривается такой субъект виктимологической защиты и профилактики, как полиция, которая в силу своих полномочий защищает личность, общество, государство от противоправных посягательств; предупреждает и пресекает преступления; выявляет и раскрывает преступления, производит дознания по уголовным делам; проводит розыск лиц; обеспечивает правопорядок в общественных местах; государственную защиту потерпевших, свидетелей и иных участников уголовного судопроизводства. Все эти действия полиция должна выполнять, когда жертвой преступления становится инвалид. В связи с цифровизацией полиция в настоящее время активно использует современные цифровые технологии, но не в полном объеме. В статье изучены вопросы и проблемы использования цифровых технологий и искусственного интеллекта при расследовании преступлений в отношении инвалидов.

Ключевые слова: право, цифровые технологии, инвалид, жертва преступления, полиция, виктимологическая профилактика и защита, преступление

POLICE AS A SUBJECT OF PREVENTION AND PROTECTION FROM CRIMINAL VICTIMITY OF DISABLED PEOPLE IN THE RUSSIAN FEDERATION IN THE CONDITIONS OF THE DIGITAL SOCIETY

Abstract. The article examines such a subject of victimological protection and prevention as the police, which, by virtue of its powers, protects the individual,

society, and the state from unlawful encroachments; prevents and suppresses crimes; identifies and solves crimes, conducts inquiries on criminal cases; conducts searches for persons; ensures law and order in public places; state protection of victims, witnesses, and other participants in criminal proceedings. All these actions the police must perform when a disabled person becomes a victim of a crime. Due to the development of digital technologies, the police are currently actively using modern trends in digital technologies, but not to the full extent. The article examines the issues and problems of using digital technologies and artificial intelligence in investigating crimes against disabled people.

Keywords: law, digital technologies, disabled person, crime victim, police, victimological prevention and protection, crime

Введение. Профилактика и защита от криминальной виктимности инвалидов в Российской Федерации является важным аспектом в современном обществе, поскольку инвалиды относятся к наиболее незащищенной категории граждан, которые могут стать жертвой преступников.

Основная часть. Одним из центральных субъектов профилактики и защиты от криминальной виктимности инвалидов в Российской Федерации выступает полиция. Полиция относится к субъектам специально-криминологического уровня системы виктимологического противодействия преступности, так как противодействие преступности путем предупреждения преступлений является их главной функциональной задачей [7. С. 60].

В силу закона основными направлениями деятельности полиции являются защита личности, общества, государства от противоправных посягательств; предупреждение и пресечение преступлений; выявление и раскрытие преступлений, производство дознания по уголовным делам; розыск лиц; обеспечение правопорядка в общественных местах; государственная защита потерпевших, свидетелей и иных участников уголовного судопроизводства (статья 2 Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции») [1].

В связи с указанными направлениями деятельности, как отмечает А. В. Аносов, работа сотрудников правоохранительных органов должна заключаться, прежде всего, в стимулировании безопасного поведения самих граждан и доведении до них элементарных правил предосторожности [3. С. 30].

При осуществлении виктимологической защиты и профилактики инвалидов целесообразно использовать широкие возможности психологической службы органов внутренних дел, поскольку при осуществлении виктимологической профилактики сотрудники органов внутренних дел сталкиваются с виктимологически сложными психологическими ситуациями при возникающей необходимости виктимологического воздействия на граждан, с которыми трудно установить психолого-педагогический контакт. Помощь профессиональных психологов можно использовать при изучении виктимологических признаков жертв преступлений, да и в каждодневной работе с конкретными гражданами [9. С. 19].

Б. П. Смагоринский и А. В. Сычева считают, что при допросе потерпевшего по делам, совершенных в отношении социально незащищенных лиц, немаловажное значение имеет установление следователем психологического контакта с допрашиваемым. Они выделяют следующие тактические приемы установления

психологического контакта: создание обстановки допроса; по возможности обеспечение отсутствия в кабинете третьих лиц; разъяснение допрашиваемому целей допроса; корректное поведение следователя (недопущение повышения голоса, употребления нецензурной брани, жаргонизмов), демонстрация его умения выслушать допрашиваемого до конца; проведение беседы на отвлеченную тему перед допросом; по возможности недопущение длительного ожидания допроса; проведение допроса в наиболее удобном для потерпевшего месте (по месту жительства, на месте совершения преступления) [8. С. 103]. А. А. Шаевич рекомендует следователям оказывать всяческую помощь лицам, дающим показания, для восстановления в памяти забытого и правильного воспроизведения воспринятого [10. С. 47].

В условиях развития цифрового общества важное значение занимают цифровые технологии и проблема доступной среды и цифровой доступности с учетом базовых общечеловеческих потребностей инвалидов [11. С. 851]. При этом стоит обратить внимание на то, что в силу развития цифровых технологий, было бы полезно разработать программу, в которой искусственный интеллект смог выступить в качестве помощника для следователя при проведении допроса (опроса) инвалида как жертвы преступления, поскольку инвалиды эмоционально уязвимые потерпевшие и нуждаются в более спокойном и уравновешенном разговоре по поводу произошедшего с ними события (преступления), но иногда допрос следователем может приобрести слишком эмоциональную направленность, что послужит «эмоциональной закрытостью» инвалида, который либо перестанет отвечать на вопросы, либо начнет путаться в показаниях и не сможет дать четкие и внятные ответы по совершенному в отношении него преступлению.

Немаловажное значение при расследовании и предупреждении преступлений в отношении инвалидов в настоящее время приобретают цифровые технологии в работе полиции.

Так, с июня 2020 г. в структуре Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации (далее – ГИАЦ МВД России) введена в эксплуатацию подсистема интегрированного банка данных федерального уровня (ИБД-Ф) «Опознавание (биометрическая идентификация)», в основе работы которой лежит принцип распознавания лиц, основанный на сверхточных нейронных сетях.

Система объединяет ресурсы дактилоскопической и фоноскопической информации, лабораторий ДНК-анализа, комплексов биометрической идентификации личности и фиксации передвижения транспортных средств, систем проверки по оперативно-справочным, розыскным и криминалистическим учетам.

Важное значение дактилоскопическая регистрация имеет для граждан, страдающих потерей памяти, особенно в тех случаях, когда они не могут сообщить о себе сведений. Регистрация позволяет найти их родственников или оказать указанным лицам своевременную медицинскую помощь [4. С. 45].

Кроме этого, ресурсы подсистема ИБД-Ф «Опознавание (биометрическая идентификация)» могут помочь и в работе с инвалидами в качестве потерпевших, так как для данных лиц в силу своих физических проблем может быть затруднительно сообщить о себе необходимые сведения и сообщить сведения о лице, совершившем преступление. В этой связи цифровые технологии в значи-

тельной степени помогут в работе полиции, а особенно может помочь искусственный интеллект.

Так, с точки зрения борьбы с преступностью и повышения общественной безопасности, как считает В. В. Агеев, искусственный интеллект имеет огромный потенциал. Эта технология может помочь в идентификации разыскиваемых лиц, угнанных транспортных средств, распознать подозрительное поведение, а также прогнозировать криминогенные тенденции в преступной среде и оптимизировать ресурсы правоохранительных органов. Кроме этого, искусственный интеллект поможет выявить аномалии в сфере финансовых операций, которые могут указывать на мошенничество, коррупцию или финансирование терроризма, выявлять запрещенный контент, распространяемый в Интернете [2].

В связи со значимостью использования искусственного интеллекта в борьбе с преступностью Министерство внутренних дел Российской Федерации планирует внедрить искусственный интеллект в правоохранительную деятельность. Ведомство собирается провести научно-исследовательскую работу и подготовить датасеты для обучения и тестирования нейросетевых моделей, а в 2025 году разработать две системы на базе искусственного интеллекта «Клон» и «Конъюктура». «Клон» позволит выявить факты подделки видеоизображений в интересах правоохранительной деятельности, «Конъюктура» должна прогнозировать негативные события и чрезвычайные ситуации и моделировать сценарии реагирования на них [6].

Также стоит отметить, что немаловажное значение в работе полиции по общению с инвалидами, являющимися жертвами преступления, имеет цифровая коммуникация. По мнению В. А. Задорожной, текущие возможности цифровой коммуникации граждан и органов расследования включают в себя: 1) подачу электронного заявления в органы, полномочные принимать и разрешать заявления о преступлениях; 2) использование видеоконференцсвязи при производстве следственных и судебных действий [5. С. 97].

Подача электронного заявления доступна через сайты МВД России, Главных управлений МВД России по субъектам Российской Федерации при выборе во вкладке «для граждан» опции «прием обращений» [5. С. 98]. Однако цифровая коммуникация потерпевших и органов расследования в настоящее время практически не используется, так как механизм использования на сегодняшний день до конца не отрегулирован и не многие граждане, а тем более инвалиды, знают о данных возможностях.

Перспективами цифровой коммуникации граждан и органов расследования, как предполагает В. А. Задорожная, выступают: введение электронного уголовного дела; создание электронных сервисов взаимодействия граждан с правоохранительными органами (подача электронных заявлений, передача в орган, ведущий производство по уголовному делу фото-видеоматериалов, документооборот, чат-бот, возможность связи со специалистом, личный кабинет, позволяющий отслеживать производство по уголовному делу [5. С. 100].

В действительности подача электронного заявления о совершенном преступлении, отслеживание рассмотрения данного заявления, отслеживание ведения уголовного дела, онлайн связь со специалистами, видео-конференц-связь при производстве следственных и судебных действий являются прекрасной пер-

спективной для расследования преступлений в отношении инвалидов, а также для активного участия самих инвалидов в следственных действиях.

Заключение. Таким образом, значение полиции как субъекта профилактики и защиты от криминальной виктимности инвалидов в Российской Федерации весьма велико. При осуществлении допроса (опроса) инвалида как жертвы преступления следователю необходимо привлекать психолога для более лучшего налаживания контакта с потерпевшим, который является инвалидом, а также рекомендуется разработка программы для использования искусственного интеллекта в качестве помощника следователю для допроса (опроса) потерпевшего-инвалида с целью исключения «человеческого фактора» и слишком эмоционального диалога следователя и потерпевшего-инвалида, так как диалог будут вести либо двое – следователь и искусственный интеллект, либо только искусственный интеллект под контролем следователя. Также необходимо разработать и внедрить в стадии расследования преступлений против инвалидов подачу инвалидами электронного заявления о совершенном преступлении и дальнейшее ведение уголовного дела в электронном виде для того, что сами инвалиды могли отслеживать процесс расследования преступления.

Список литературы

1. О полиции: Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (в ред. от 08.08.2024 г.) // Собрание законодательства Российской Федерации. 2011. № 7. – Ст. 900.
2. Агеев В. В. Большие данные и искусственный интеллект на службе полиции // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сборник статей Международной научно-практической конференции / ответственный за выпуск В. О. Лапин. М.: Академия управления МВД России, 2019. С. 11–13.
3. Аносов А. В. Организационные аспекты виктимологической профилактики преступлений, совершаемых с использованием информационных технологий // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2019. № 1 (55). С. 28–31.
4. Вихляев А. А., Калинина С. В. Приоритетные направления деятельности и основные элементы информационно-аналитической работы подразделений ГИАЦ МВД России в условиях цифровизации органов внутренних дел // Научный портал МВД России. 2023. № 1 (61). С. 43–48.
5. Задорожная В. А. Цифровая коммуникация граждан и органов расследования: влияние на защиту потерпевших от преступлений // Защита жертв преступлений в современном обществе (PVCMS 2023): материалы VI Международной научно-практической интернет-конференции (Челябинск, 21–22 февраля 2023 г.) / отв. ред. А. В. Майоров. Челябинск: Эскуэла, 2023. С. 94–101. URL: <https://victimolog.ru/index.php/PVCMS/article/view/533>
6. Кинякина Е., Устинова А. МВД привлечет нейросети к поиску правонарушителей // URL: <https://www.vedomosti.ru/technology/articles/2024/01/11/1014513-mvd-privlechet-neiroseti-k-poisku-pravonarushitelei> (дата обращения 29.08.2024 г.).
7. Майоров А. В. Содержание системы виктимологического противодействия преступности // Юридическая наука и правоохранительная практика. 2017. № 3. С. 56–65.

8. Смагоринский Б. П., Сычева А. В. Специфика расследования мошенничеств, совершенных в отношении социально незащищенных лиц в современных условиях // Научный портал МВД России. 2022. № 1 (57). С. 98–105.

9. Сплавская Н. В. Организационное и информационное обеспечение виктимологической профилактики, осуществляемой органами внутренних дел // Государство и право в XXI веке. 2014. № 2. С. 19–22.

10. Шаевич А. А. О проблемах установления психологического контакта при производстве отдельных следственных действий // Научный портал МВД России. 2018. № 2 (42). С. 45–51.

11. Хатсон Д., Хатсон П. Цифровая инклюзия для людей с расстройствами аутистического спектра: пересмотр существующих правовых моделей и доктринальных концепций // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 851–879. EDN: aorqmxu

Р. Н. Малышкин,
кандидат юридических наук,
Казанский инновационный университет
имени В. Г. Тимирязова,
И. В. Слепнева,
студент,
Казанский инновационный университет
имени В. Г. Тимирязова

О ВОПРОСАХ КВАЛИФИКАЦИИ КРАЖИ С БАНКОВСКОГО СЧЕТА, А РАВНО В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

Аннотация. В статье рассматривается п. «г» ч. 3 ст. 158 УК РФ – кража с банковского счета, а равно в отношении электронных денежных средств. В 2018 году ч. 3 ст. 158 УК РФ была дополнена п. «г», который устанавливает уголовную ответственность за кражу с банковского счета и электронных денежных средств при отсутствии признаков преступления, предусмотренных ст. 159.3 УК РФ. Также утверждается, что данный квалифицирующий признак нарушает принцип справедливости и отрицательно влияет на состояние судимости в России. Отмечается, что хищение электронных денежных средств несет большую общественную опасность, нежели хищение, предусмотренное ч. 1 ст. 158 УК РФ. Однако не согласны с квалификацией законодателя.

Ключевые слова: право, цифровые технологии, кража с банковского счета, кража электронных денежных средств, финансовые технологии, квалифицирующие признаки кражи, принцип справедливости

ON QUESTIONS OF QUALIFICATION OF THEFT FROM A BANK ACCOUNT, AS WELL AS IN RELATION TO ELECTRONIC MONEY

Abstract. The article examines paragraph "g" of Part 3 of Article 158 of the Criminal Code of the Russian Federation – theft from a bank account, as well as in relation to electronic money. In 2018, Part 3 of Article 158 of the Criminal Code of the Russian Federation was supplemented with paragraph "g", which establishes criminal

liability for theft from a bank account and electronic money in the absence of elements of a crime provided for in Article 159.3 of the Criminal Code of the Russian Federation. It is also argued that this qualifying feature violates the principle of justice and negatively affects the status of a criminal record in Russia. The authors believe that theft of electronic money poses a greater public danger than theft provided for in Part 1 of Article 158 of the Criminal Code of the Russian Federation. However, they do not agree with the qualification of the legislator.

Keywords: law, digital technologies, theft from a bank account, theft of electronic funds, financial technologies, qualifying features of theft, the principle of fairness

Введение. Российская Федерация находится в лидерах по использованию безналичных денежных средств. Еще десять лет назад оборот наличных денег в стране был в разы выше нынешнего. На сегодняшний день доля наличных денежных средств составляет лишь 16,8%, тогда как в начале двухтысячных эта цифра составляла 35% [1]. Граждане привыкают обходиться без наличных денег. Также развиваются способы расчетов при помощи безналичных платежей, использование электронных средств оплаты, что влечет новые проблемы.

Основная часть. В условиях стремительного развития финансовых технологий и увеличения объемов онлайн-транзакций, вопросы безопасности и защиты личных данных становятся особенно актуальными. Так в 2018 году ч. 3 ст. 158 УК РФ была дополнена п. «г» [6]. С момента внесения изменений и по сегодняшний день п. «г» ч. 3 ст. 158 УК РФ предусматривает уголовную ответственность за совершение кражи «с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 настоящего Кодекса)» [5].

Внесение изменений в ч. 3 ст. 158 УК РФ было на тот момент достаточно ожидаемым, даже оправданным. Стремительный рост хищений денежных средств с банковских карт затрагивал все большее число людей и вызывал недовольство. А лица совершающие хищения, напротив, считали себя в безопасности, поскольку совершали преступление дистанционно и были уверены в своей безнаказанности. Поэтому законодатель решилкратно увеличить ответственность за хищение электронных денежных средств.

Однако мы с таким решением законодателя не можем согласиться в полной мере. По нашему мнению, наличие данного квалифицирующего признака противоречит принципам уголовного права, в первую очередь принципу справедливости, а также пагубно влияет на состояние судимости в России.

В ч. 3 ст. 158 УК РФ содержатся следующие квалифицирующие признаки, устанавливающие уголовную ответственность за кражу:

- с незаконным проникновением в жилище;
- из нефтепровода, нефтепродуктопровода, газопровода;
- в крупном размере;
- с банковского счета, а равно в отношении электронных денежных средств.

То есть законодатель ставит все вышеперечисленное в один ряд и считает, что общественная опасность от каждого из деяний является равной (или почти

равной). Мы с этим в корне не согласны и вот почему. Для квалификации деяния по ч. 1 ст. 158 УК РФ достаточно совершить тайное хищение чужого имущества на сумму, превышающую 2 500 рублей. Для квалификации деяния по п. «в» ч. 2 ст. 158 УК РФ – не менее 5 000 рублей. Таким образом, хищение 3 000 рублей из физического кошелька потерпевшего наказывается лишением свободы до двух лет, а кража денежных средств с виртуального кошелька – до шести лет лишения свободы. В данной ситуации законодатель явно не предполагал, что общественная опасность кражи с банковского счета будет выражаться в количестве похищенных денежных средств. Значит, нужно обратить внимание не на количественные, а качественные квалифицирующие признаки.

Повышенная общественная опасность кражи с незаконным проникновением в жилище, а также в нефтепроводы и газопроводы кажется нам вполне логичным. Проникновение в любое из ранее названных помещений (сооружений) ставит под удар не только общественные отношения, охраняющие право собственности и иные вещные права, но и право на жизнь, здоровье.

Аргумент в защиту квалифицирующего признака, предусмотренного п. «г» о том, что его повышенная опасность обусловлена риском использования вредоносных программ, считаем несостоятельным. Поскольку в данной ситуации деяния будут квалифицироваться по совокупности преступлений (п. «г» ч. 3 ст. 158 и соответствующей части ст. 273 УК РФ).

Верховный Суд Российской Федерации в своем постановлении также косвенно подмечает повышенную общественную опасность данного деяния. По общему правилу, кража считается оконченной, когда имущество было изъято, и виновного лица появилась реальная возможность распорядиться этим имуществом. Однако «кража с банковского счета считается оконченной с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб» [4]. Данное уточнение нам кажется особенно интересным, поскольку оно кардинально меняет сложившуюся в течение предыдущих десяти лет судебную практику в области определения момента окончания преступления [1].

А. В. Креховец проанализировав судебную практику в различных регионах России по п. «г» ч. 3 ст. 158 УК РФ также приходит к выводу о нарушении принципа справедливости [3].

В связи с этим следует отметить, что хищение электронных денежных средств носит большую общественную опасность, чем хищение, скажем, кошелька из кармана куртки. Однако мы считаем, что законодатель уровень общественной опасности сильно завысил. О повышенной общественной опасности нам говорит способ совершения хищения. Хищение имущества (в том числе денег), совершенное физическим воздействием относительно примитивно, иными словами, не требует особых навыков и интеллектуальных способностей. Хищение электронных денежных средств предполагает, что лицо задолго до совершения преступления начинает к нему тщательно готовиться: собирает информацию, изучает работу специальных компьютерных программ, выискивает уязвимые места в работе банковских систем и приложений. Таким образом, такой преступник нанесет больший ущерб гражданам, финансовым организациям и государству.

Кроме этого, мы исходим из того, что хищение из кошелька, неважно физического или электронного, воспринимается потерпевшим одинаково. И то, и другое деяние – покушение на его неприкосновенность. Однако нарушение неприкосновенности вследствие хищения электронных денежных средств представляет меньшую общественную опасность, чем хищение с проникновением в жилище, нефтехранилище и т. п.

Исходя из вышесказанного, мы считаем, что наличие п. «г» в ч.3 ст. 158 УК РФ неоправданно. Соответственно его из данной части следует исключить. Поскольку общественная опасность хищений электронных денежных средств выше, чем у простого хищения, предусмотренного ч.1 ст. 158 УК РФ, то полное исключение данного квалифицирующего признака приведет к тому, что соответствующее преступление будут квалифицировать по его размеру, а это также не будет в полной мере отражать всю общественную опасность.

Одним из возможных вариантов нам видится следующий: внесение квалифицирующего признака «с банковского счета, а равно в отношении электронных денежных средств» в ч. 2 ст. 158 УК РФ, т. е. в разряд преступлений средней тяжести. А также дополнить ч. 3 ст. 158 УК РФ новым квалифицирующим признаком «с банковского счета, а равно в отношении электронных денежных средств, совершенных в крупном размере».

Список литературы

1. Алехин В. П., Булавка Д. М. Проблемы квалификации хищения электронных денежных средств // Эпомен. 2019. № 34. С. 20–25.
2. Интернет-портал «Российской газеты» [Электронный ресурс]. URL: <https://rg.ru/turbopages.org/turbo/rg.ru/s/2024/04/02/na-minornoj-banknote.html> (дата обращения: 07.09.2024).
3. Креховец А. В., Степанова М. А., Царев Е. В. Проблемы квалификации преступления // Вестник Российского нового университета. Серия: Человек и общество. 2021. № 1. С. 158–165.
4. О судебной практике по делам о краже, грабеже и разбое: Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 15.12.2022) // Бюллетень Верховного Суда Российской Федерации. 2003. № 2.
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 08.08.2024) // Собрание законодательства Российской Федерации. 17.06.1996. № 25, ст. 2954.
6. О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 23.04.2018 № 111-ФЗ // Собрание законодательства Российской Федерации. 2018. № 18, ст. 2581.

Л. Р. Хайрутдинова,
старший преподаватель,
Казанский инновационный университет
имени В. Г. Тимирязова

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ КВАЛИФИКАЦИИ И ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ КИБЕРГРУМИНГА КАК ПРЕСТУПЛЕНИЯ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ НЕСОВЕРШЕННОЛЕТНИХ

Аннотация. В представленной статье проводится характеристика такого преступного явления, как кибергруминг, который требует научного осмысления. Данное преступное деяние характеризуется тем, что преступником чаще всего является лицо, достигшее совершеннолетнего возраста, который выстраивает эмоциональную связь с несовершеннолетней жертвой в виртуальной среде с целью сексуального насилия или иной эксплуатации.

Ключевые слова: несовершеннолетние, виктимность, жертва, половая неприкосновенность, кибергруминг, преступление

PROBLEMS OF CRIMINAL LAW QUALIFICATION AND LAW ENFORCEMENT PRACTICE OF CYBERGRUMING AS CRIMES AGAINST THE SEXUAL INTEGRITY OF MINORS

Abstract. The presented article characterizes such a criminal phenomenon as “cybergrooming,” which requires scientific understanding. This criminal act is characterized by the fact that the offender is most often a person who has reached the age of majority, who builds an emotional connection with a minor victim in a virtual environment for the purpose of sexual violence or other exploitation.

Keywords: minors, victimhood, victim, sexual integrity, cybergrooming, crime

Введение. В настоящее время использование Интернета в киберпространстве является необходимостью в любой деятельности. Система ценностей в обществе меняется, и локально-частные ценности становятся глобально-универсальными. В итоге это приведет к глобальному изменению в ценностях, нормах права и морали [1]. В своей деятельности юристы неизбежно сталкиваются с новыми феноменами, порождаемыми цифровизацией [9. С. 258].

Основная часть. Развитие новых технологий оказывает на людей положительное и отрицательное воздействие. Одним из положительных факторов можно отметить, доступность информации для обучения, работы, общения без необходимости разговаривать лично друг с другом и вне зависимости от местоположения. В то же время социальные сети являются одними из способов совершения преступлений [2. Р. 5; 8]. Ребенок может невольно становится жертвой киберпреступности. К примеру, груминг означает «ухаживать» и метафорически обозначает тонкий подход преступников к детям и молодым людям.

Исследования показывают, что люди в возрасте от 18 до 23 лет часто не осознают процесс груминга. Они часто вступают в отношения с грумерами, не осознавая применяемых обманных и манипулятивных приемов, ошибочно вос-

принимая эти отношения как добровольные, а не оскорбительные [4]. По своей сути, груминг означает виртуальную обработку ребенка взрослым преступником для достижения собственных целей. В своем наиболее популярном значении он относится к сексуальной виктимизации детей, когда взрослый дружит с несовершеннолетним и выстраивает эмоциональную связь с целью сексуального насилия, эксплуатации и даже торговли такой жертвой. Сексуальное домогательство в отношении детей и подростков, реализуемое в форме кибергруминга, стало одной из опаснейших угроз для их оптимального психического развития [5. С. 416]. Появление технологий переместило физическую близость преступников в Интернет, что позволило груммерам полностью интегрироваться в жизнь жертвы, поддерживая постоянный контакт. Отмечается, что, хотя груминг может происходить как в сети, так и в реальной жизни, грумеры часто устанавливают онлайн-контакт, прежде чем перевести «отношения» в офлайн для совершения сексуальных преступлений.

Груминг не ограничивается сексуальной эксплуатацией, так как развитие технологий расширило влияние экстремистских идеологических групп, предоставив им доступ к детям, которых можно принудить принять их убеждения. Это явление, известное как идеологический груминг, представляет собой значительные личные, социальные, национальные и правоохранные проблемы. Кроме того, новая тенденция, называемая цифровым коммерческим грумингом, подразумевает, что злоумышленники манипулируют несовершеннолетними, чтобы они приобретали и употребляли наркотики.

Согласно Уголовному кодексу РФ объективная сторона статей 131–135 не предусматривает ответственность за виртуальное общение с несовершеннолетним с последующей сексуальной целью. Хотя такая форма сексуального насилия, например, наказуема в Германии (§ 176a и 176b StGB). Кибергруминг может привести к тюремному заключению на срок от трех месяцев до пяти лет или от шести месяцев до десяти лет [5].

Кибергруминг характеризуется определенными стратегиями преступников, которые часто схожи. Все они основаны на эксплуатации невежества, доверчивости и отсутствия осознания риска у детей и подростков. Преступники часто пытаются установить доверительные отношения, чтобы в дальнейшем контролировать своих жертв и манипулировать ими.

Кибергруминг – это целенаправленное инициирование сексуального контакта чаще всего взрослого с несовершеннолетними через Интернет, который знакомится с ребенком в сети и выстраивает эмоциональную связь с будущими намерениями сексуального насилия, сексуальной эксплуатации или торговли людьми. Преступники ищут своих жертв на популярных платформах, таких как TikTok, Instagram¹¹, Facebook¹², Snapchat, или в видеоиграх, выдавая себя за детей или молодых людей того же возраста в чатах или онлайн-сообществах, чтобы изначально выстроить доверие ничего не подозревающих несовершеннолетних

¹¹ Социальная сеть принадлежит Meta, признана в России экстремистской.

¹² Социальная сеть принадлежит Meta, признана в России экстремистской.

[6. С. 306], а затем манипулировать ими. Их цель обычно состоит в том, чтобы встретиться с несовершеннолетними жертвами в «реальном» мире и совершить преступления против их половой неприкосновенности. Преступники часто могут убедить несовершеннолетних заранее отправить им откровенные фотографии. Затем используют их в качестве шантажа, как средство давления на несовершеннолетних, чтобы они совершили дальнейшие действия сексуального характера.

Главные цели кибергруминга – завоевать доверие ребенка, получить интимные и личные данные от ребенка (сексуального характера, интимные разговоры, фотографии или видео) с последующим использованием в преступных целях.

Таким образом, количество преступлений, которые совершаются с помощью сети «Интернет» возрастает и само явление кибергруминг демонстрирует, как преступники используют Интернет и смартфоны для совершения преступлений особенно в отношении несовершеннолетних. В связи с чем необходимо внести изменения в главу 18 «Преступления против половой неприкосновенности и половой свободы личности» [7] с дополнением пунктом о сексуальном преследовании с использованием сети Интернет.

В качестве рекомендаций по профилактике преступлений в сети Интернет, необходимо проводить беседы с детьми, чтобы они не сообщали в чатах и социальных сетях свои личные данные. В том числе следить за тем, чтобы дети ответственно обращались со своими фотографиями и видеофайлами и не публиковали без одобрения от родителей. Обсудить с детьми разницу между «другом» в реальной жизни и «другом» в виртуальном мире. Родителям и учителям необходимо общаться с детьми по вопросам использования сети Интернет, использования социальных сетей и обсуждать с ними потенциальные риски и их последствия. Обязательно принять меры по конфиденциальности в социальных сетях для несовершеннолетних, чтобы обезопасить их личную информацию и сделать ее недопустимой для посторонних пользователей. Интегрировать систему искусственного интеллекта для отслеживания кибергруминга и киберсталкинга [9. С. 133] в отношении несовершеннолетних.

Список литературы

1. Анненкова И. В., Залоило М. В. Новая культура коммуникаций в условиях цифровой и социокультурной глобализации: право, медиа и национальная идентичность // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 3. С. 140–155.
2. Anjeli Holivia, Teguh Suratman. Child cyber grooming sebagai bentuk modus baru cyber space crimes // Bhirawa Law Journal Volume 2, issue 1, May 2021. – P. 1-13.
3. Arundhati Kale. Cyber Grooming: An Increasing Threat // [https://www-cyberpeace-org](https://www.cyberpeace-org).
4. Медведева А. С., Дозорцева Е. Г. Влияние родителей на процесс кибергруминга // Цифровая гуманитаристика и технологии в образовании (DHTE 2021): сб. статей II Всероссийской научно-практической конференции с международным участием. 11–12 ноября 2021 г. / Под ред. В.В. Рубцова, М.Г. Сороковой, Н.П. Радчиковой. М.: Издательство ФГБОУВОМГППУ, 2021. – С.415–424.

5. Ein Service des Bundesministeriums der Justiz sowie des Bundesamts für Justiz – www.gesetze-im-internet.de.

6. Хайрутдинова Л. Р. Обеспечение безопасности детей в интернет-пространстве: причины и проблемы реализации // В сборнике: Цифровые технологии и право. сборник научных трудов II Международной научно-практической конференции В 6 т. Казань, 2023. С. 306–308.

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

8. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.

9. Виноградова А. А., Хайрутдинова Л. Р. Кибервиктимность жертв киберсталкинга // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции. В 6 т. / под ред. И. Р. Бегишева [и др.]. Казань, 2022. – С. 133–135.

А. А. Шутова,
кандидат юридических наук,
Казанского инновационного университета
имени В. Г. Тимирязева

КОНЦЕПЦИЯ ЦИФРОВОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ КАК ФЕНОМЕНА, ЗНАЧИМОГО ДЛЯ УГОЛОВНОГО ПРАВА

Аннотация. Цель статьи – сформировать концепцию цифровой безопасности системы здравоохранения как феномена, значимого для уголовного права. Процедура и методы: в процессе исследования использовались общенаучные (анализ, синтез, индукция, дедукция) и частнонаучные методы научного познания. Результаты: по итогам исследования сформированы элементы цифровой безопасности системы здравоохранения. Кроме того, сформирован понятийно-категориальный аппарат, который, по нашему мнению, расширит отечественную науку и может быть использован при совершенствовании действующего законодательства, даны определения понятиям «здравоохранение», «цифровое здравоохранение», «цифровая безопасность системы здравоохранения», «цифровая угроза» и «обеспечение цифровой безопасности системы здравоохранения». Теоретическая и/или практическая значимость данного исследования состоит в его теоретико-прикладной направленности, которая в целом позволит повысить систему мер реагирования на преступления, совершаемые против цифровой безопасности системы здравоохранения, а также позволит сформировать концепцию цифровой безопасности системы здравоохранения как феномена, значимого для уголовного права.

Ключевые слова: цифровое здравоохранение, цифровая медицина, цифровая безопасность, преступления, цифровые технологии, биомедицинские технологии

THE CONCEPT OF DIGITAL SECURITY OF THE HEALTHCARE SYSTEM AS A PHENOMENON SIGNIFICANT FOR CRIMINAL LAW

Abstract. Aim. To form the concept of digital security of the healthcare system as a phenomenon significant for criminal law. Methodology. In the course of the research, general scientific (analysis, synthesis, induction, deduction) and private scientific methods of scientific cognition were used. Results. Based on the results of the study, the elements of digital security of the healthcare system were formed. In addition, a conceptual and categorical apparatus has been formed, which, in our opinion, will expand domestic science and can be used to improve current legislation, definitions of the concepts of "healthcare", "digital healthcare", "digital security of the healthcare system", "digital threat" and "ensuring digital security of the healthcare system" are given. Research implications. This research consists in its theoretical and applied orientation, which in general will improve the system of measures to respond to crimes committed against the digital security of the health care system, and will also form the concept of digital security of the health care system as a phenomenon significant for criminal law.

Keywords: digital healthcare, digital medicine, digital security, crime, digital technologies, biomedical technologies

Введение. Распространение новейших цифровых технологий во всех сферах жизнедеятельности человека не смогли оставить сферу здравоохранения незатронутой и не подверженной их влиянию. Многие исследователи полагают, что, начиная от мобильных медицинских приложений и программного обеспечения, поддерживающих принятие клинических решений медицинскими работниками, и до искусственного интеллекта и машинного обучения, цифровые технологии произвели революцию в традиционной медицинской практике [1]. Цифровое здравоохранение способно предотвращать заболевания и тем самым снижать затраты на предоставляемые медицинские услуги, одновременно помогая пациентам контролировать, диагностировать и лечить хронические заболевания [2], а также адаптировать лекарства для конкретных больных граждан. В медицине традиционные методы диагностики вытесняются методами цифровыми, что привело к тому, что почти каждый компонент медицинской сферы находится в процессе оцифровки [3].

Наряду с этим сфера цифрового здравоохранения подвержена многочисленным криминальным посягательствам и не оставляет злоумышленников равнодушными. Поэтому считаем то, что запрос на уголовно-правовую охрану цифровой безопасности системы здравоохранения *обусловлен целым комплексом причин:*

- ускоренными темпами развития цифровых технологий в сфере здравоохранения;
- достаточно новым характером многих сквозных цифровых технологий, последствия применения которых еще только прогнозируются и правовое регулирование которых начинает закладываться;

- здравоохранение в целом направлено на охрану жизни и здоровья граждан, которые являются наивысшими ценностями, что обуславливает потребность в их особой защите и охране;
- повышенной общественной опасностью противоправных деяний в этой сфере и значительными негативными последствиями, которые могут быть причинены в результате их совершения;
- здравоохранение является привлекательной отраслью для киберпреступников, поскольку медицинские данные бывают даже ценнее, чем данные кредитных карт или банковские данные. Незаконным образом полученные медицинские записи могут быть проданы для финансирования преступной деятельности и облегчения незаконного получения личных данных, шантажа или вымогательства. Сведения о состоянии здоровья пациентов обычно сопровождаются личной информацией, которую можно незаконно покупать или продавать;
- медицинские устройства, оснащенные цифровыми технологиями, могут быть взломаны или захвачен их доступ, что не позволит медицинским организациям предоставлять необходимое лечение пациентам и может в целом привести к летальным последствиям.

По нашему мнению, указанные причины обуславливают потребность и необходимость в уголовно-правовой охране цифровой безопасности системы здравоохранения.

Предпосылки цифровой трансформации системы здравоохранения. На данный момент следует констатировать вектор развития государственной политики Российской Федерации, направленной на форсированную цифровизацию здравоохранения. Действующие нормативные правовые акты Российской Федерации уже детальным образом регулируют одно из важнейших направлений – стратегию цифровой трансформации здравоохранения. Так, распоряжением Правительства Российской Федерации от 29 декабря 2021 г. № 3980-р определено стратегическое направление в области цифровой трансформации здравоохранения до 2024 года [4]. Основаниями разработки данного стратегического направления является множество нормативных правовых актов, регламентирующих отдельные правления и этапы подобного инновационного развития [5–8]. Принятие указанных документов демонстрирует то, что цифровизация оказывает активное влияние на систему здравоохранения.

На данный момент к предпосылкам цифровой трансформации системы здравоохранения следует отнести:

во-первых, достижения в науке и клинической медицине, цифровых технологий в здравоохранении предоставляют возможность разрабатывать новые и ранее неизвестные методы диагностики и лечения пациентов, которые могут быть весьма эффективны;

во-вторых, на данный момент многими пациентами уже активно используются различные инструменты («гаджеты») и иные мобильные устройства в процессе оказания им медицинской помощи;

в-третьих, большие расстояния между некоторыми населенными пунктами, не позволяющими оказывать быстро и качественно первичную медико-санитарную и иные виды высокотехнологичной помощи, вызывают необходимость развивать цифровые технологии в здравоохранении;

в-четвертых, одним из курсов современной медицинской практики является пациенториентированность, состоящая в выборе индивидуального мониторинга и метода лечения, при этом пациент активно участвует в сборе данных, ознакомлении с информационными ресурсами, выборе врача и метода лечения, выборе стоит ли к нему применять цифровые технологии;

в-пятых, специалистами отмечается такая причина, как старение населения и рост продолжительности жизни, что повлияет на изменение существующей системы здравоохранения и повлечет необходимость ее цифровизации для обеспечения устойчивости [9. С. 125].

Стоит согласиться с мнением авторов, полагающих то, что уже сейчас стратегия на цифровую трансформацию – это не просто желательность, а основной вектор и имеющаяся необходимость нашего государства [10. С. 7]. Подобная тенденция связана с тем, что жизнь и здоровье людей являются наиболее важными ценностями, а их гарантия и защита – в первую очередь обязанностью государства. В связи с этим государство, как основной регулятор предоставления медицинских услуг, должно быть заинтересовано в том, чтобы оказывать эти услуги качественно и своевременно, поскольку от них зависят основные охраняемые блага.

На необходимость ускоренной цифровизации сферы здравоохранения неоднократно указывал и Президент Российской Федерации В. В. Путин, который еще в 2018 г. уточнил: «Мы сделаем отдельную программу по цифровизации здравоохранения» [11].

Понятие цифрового здравоохранения. В настоящее время нет единого мнения по определению понятия цифровое здравоохранение. Например, термин «цифровая медицина» при первом впечатлении напоминает цифровое здравоохранение, поскольку он также относится к использованию цифровых технологий для совершенствования и индивидуализации медицины [12. С. 133]. Поэтому цифровое здравоохранение часто рассматривают как понятие, тождественное электронному здравоохранению, мобильному здравоохранению (mHealth), телемедицине и телездоровоохранению [13; 14]. Однако полагаем, что указанная двусмысленность требует разработки всеобъемлющего определения, охватывающего различные термины, которые могут использоваться для описания цифрового здравоохранения.

Одним из аргументов, подтверждающих возможность использования термина «цифровизация здравоохранения», является его употребление в нормативных правовых актах [15].

В Глобальной стратегии в области цифрового здравоохранения цифровое здравоохранение определяется как «область знаний и практики, связанная с развитием и использованием цифровых технологий для улучшения здоровья» [16], покрывая тем самым весь спектр применения высокотехнологичных устройств в решении задач охраны здоровья граждан, включая Интернет вещей, искусственный интеллект, робототехнику и другие.

Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США (FDA) рассматривает цифровое здравоохранение как совокупность мобильного здравоохранения, носимых устройств, телездоровоохранения, телемедицины, персонализированной медицины, электронных медицинских записей и медицинских информационных технологий [17].

Следует отметить, что несмотря на то, что термин «цифровизация» часто встречается в действующих нормативных правовых актах, он не получил своего легального определения в нормах федерального закона. Определение «цифровизация» закреплено приказом Минкомсвязи России от 1 августа 2018 г. № 428 «Об утверждении Разъяснений (методических рекомендаций) по разработке региональных проектов в рамках федеральных проектов национальной программы «Цифровая экономика Российской Федерации» [18], в котором понятия «цифровизация» и «цифровое развитие» отождествлены и под ними понимается «процесс организации выполнения в цифровой среде функций и деятельности (бизнес-процессов), ранее выполнявшихся людьми и организациями без использования цифровых продуктов».

В 2017 г. Указом Президента Российской Федерации утверждена Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, определены несколько областей работы, одним из которых является цифровое здравоохранение – использование информационных и коммуникационных технологий для решения вопросов здравоохранения [19].

Среди авторов существует значительное количество точек зрения относительно определения понятия цифровое здравоохранение. Так, С. И. Коданева под цифровым здравоохранением понимает в основном применение цифровых технологий, которые используются в процессе оказания медицинской помощи населению, в том числе сервисы дистанционного взаимодействия врача и пациента, систему использования устройств, позволяющих осуществлять удаленный мониторинг жизненных показателей и т. д. [20. С. 617].

В свою очередь А. А. Карцхия под цифровым здравоохранением понимает сферу, оказываемую с помощью цифровых технологий самого широкого профиля, начиная от телемедицины, заканчивая машинным обучением и искусственным интеллектом, в целом предназначенных для оказания медицинской помощи (услуг) населению [21]. Данное определение значительным образом детализирует возможности цифровых технологий в здравоохранении, их значительную роль, однако оставляет без внимания иные составляющие цифровой безопасности системы здравоохранения (цифровую безопасность информации и инфраструктуры учреждений системы здравоохранения).

Ряд специалистов к цифровому здравоохранению относят подотрасль здравоохранения, которая обеспечивает сохранение и укрепление здоровья населения, в том числе предоставление медицинской помощи [10. С. 9]. Полагаем, что данное определение, несмотря на его объемность, не позволяет охарактеризовать сущность цифрового здравоохранения, его признаки и специфические черты.

Мы понимаем под термином «цифровое здравоохранение» множество форм реализации, к которым следует отнести:

- средства взаимодействия (удаленная диагностика пациента, дистанционное обучение медицинских работников, проведение онлайн конференций, повышения квалификации, иные сообщества пациентов и ассоциации врачей);
- системы обратной связи (персонализированный мониторинг, мобильные приложения и иные формы дистанционных консультаций, в том числе онлайн);
- технологические инструменты (портативный госпиталь, биопринтинг, системы самонаблюдения).

Итак, цифровое здравоохранение – междисциплинарная область, целью которой является повышение эффективности мониторинга пациентов, диагностики, ведения, профилактики, реабилитации и оказания медицинской помощи за счет использования цифровых технологий, средств и методов их обеспечения.

Таким образом, возможности применения цифровых технологий в сфере здравоохранения разнообразны и могут быть связаны с информационными технологиями, включая электронные услуги, ориентированные в основном на пациентов, например, запись на прием к врачу; проверка списков ожидания; доступ к соответствующей медицинской помощи из дома; обмен информацией с другими людьми с такими же проблемами со здоровьем; и доступ к персонализированной и квалифицированной медицинской информации [22]. К ним относятся использование дополненной реальности в качестве поддержки принятия клинических решений, удаленная диагностика, помощь по назначению медицинских рецептов на основе Интернета вещей, роботы для сложных медицинских процедур, цифровые неинвазивные медицинские методы или облачное прогнозирование состояния пациента в реальном времени [23].

Внедрение цифровых технологий в систему здравоохранения преобразует традиционные способы работы и взаимодействия, а также трансформацию отечественного законодательства. Успех стратегий и инструментов цифрового здравоохранения зависит от их принятия врачами и пациентами, и косвенно – от способа реализации таких стратегий.

Цифровое здравоохранение – это широкая междисциплинарная концепция, возникшая на стыке цифровых технологий и здравоохранения, представляющая под собой область знаний и практики, связанную с разработкой и использованием цифровых технологий, а также средств и методов ее обеспечения (цифровой информации и цифровой инфраструктуры) в учреждениях системы здравоохранения.

Цифровизация системы здравоохранения породила множество проблем, начиная от недостаточной цифровой грамотности среди пациентов и заканчивая сложностями, связанными с хранением данных, доступом, обменом и владением ими. Подобные опасения, в свою очередь, поднимают вопросы безопасности и конфиденциальности, если, к примеру, медицинские устройства будут взломаны. Дополнительные проблемы связаны с технологиями и этикой. Например, возникают вопросы, связанные с тем, кто при использовании медицинских роботов будет нести ответственность за ошибки, допущенные во время операции: больница, разработчик или производитель технологии, врач, использовавший робота, или кто-то другой?

Одновременно с этим процесс цифровизации привел к росту мошенничества и совершению иных преступлений против цифровой безопасности системы здравоохранения. На черном рынке можно легко получить доступ к более чем 1 миллиарду медицинских записей пациентов, и ежедневно добавляются миллионы дополнительных записей [24]. С 2016 г. сфера здравоохранения стала жертвой большего количества атак кибербезопасности, чем даже финансовая отрасль [25]. По результатам проведенных исследований последствия вспышек кибератак во время COVID-2019 оказали сильнейшее влияние на 2 сектора: на здравоохранение и на банковскую сферу [26]. Кража личных медицинских данных

растет, поскольку эти записи стоят больше, чем записи любой другой отрасли, из-за высокой ценности личной информации. Как следствие, здравоохранение значительно отстает от других сфер в своей способности защитить критически важные данные. Однако отказ от обслуживания в учреждениях системы здравоохранения может привести в худшем случае – к полному прекращению операций, что окажет серьезное влияние на ценность здравоохранения. Следовательно, последствия от кибератаки могут повлечь наступление негативных последствий в связи с тем, что оказание медицинских сильно зависит от цифровых решений.

Кибербезопасность в здравоохранении определяется как проблема безопасности здравоохранения. Учитывая важность цифрового здравоохранения и его потенциал, необходимо, чтобы меры кибербезопасности были соизмеримы с рисками, с которыми сталкивается медицина.

Сфера цифрового здравоохранения может быть объектом преступных посягательств как со стороны медицинских работников, так и обычных граждан, которые не имеют медицинского образования, однако их противоправные намерения непосредственно причиняют вред организации системы здравоохранения. Несомненно, в некоторых случаях действия виновных могут быть направлены на достижение корыстных целей, однако осуществляют их посредством воздействия на учреждения системы здравоохранения. Изучение подобных материалов позволяет утверждать то, что противоправные посягательства осуществляются с целью получения денежных средств или криптовалюты за расшифровку данных или предоставления доступа к заблокированной информации [27. С. 134]. Совершение преступлений в сфере здравоохранения остается весьма на высоком уровне, а в свете перехода на цифровое здравоохранение криминальные риски и угрозы растут еще больше, поскольку любая технология имеет перспективу своей эксплуатации в преступных целях [28. С. 652].

Цифровая безопасность системы здравоохранения. В связи с форсированной цифровизацией системы здравоохранения, государству будет необходимо обеспечивать достойный уровень ее безопасности в подобных условиях развития общественных отношений от нарастающих угроз. В условиях стремительного роста цифровых технологий, применяемых в сфере здравоохранения, увеличения массива данных и повышения их значения (в связи с необходимостью обучения алгоритмов искусственного интеллекта), необходимости их передачи и обработки в цифровой форме, достаточно актуальными становятся вопросы обеспечения безопасности цифровой информации, образующейся в учреждениях системы здравоохранения, цифровой инфраструктуры учреждений системы здравоохранения и цифровых технологий, используемых в системе здравоохранения. В связи с этим вопросам безопасности системы здравоохранения должно отводиться большое значение. Несомненно, безопасность – это комплексное понятие [29]. В нормативных правовых актах под термином безопасность понимается состояние защищенности жизненно важных интересов личности, общества и государства [30], национальных интересов [31], или участников дорожного движения [32] от каких-либо угроз. В исследовании мы планируем придерживаться позиции, уже сложившейся в национальной правовой системе России, относительно определения понятия «безопасность».

В действительности, вопросам безопасности системы здравоохранения должно отдаваться первостепенное значение особенно в свете роста количества преступлений, совершаемых в цифровом пространстве. Кроме того, пациенты должны продолжать получать медицинскую помощь после совершения уголовно наказуемых деяний на медицинские учреждения, так как от этого может зависеть их жизнь и здоровье.

В связи с этим особое место должно отдаваться охране цифровой инфраструктуры системы здравоохранения, которая нуждается в кибербезопасности для защиты конфиденциальности, безопасности и жизни пациентов. В настоящее время программные инструменты не справляются с обнаружением новых киберугроз и защитой медицинских учреждений, что приводит к техническому провалу. За последнее время киберпреступники атаковали сектор здравоохранения и использовали программы-вымогатели для предотвращения доступа к критически важным системам и данным. В результате подобных криминальных посягательств учреждения системы здравоохранения были вынуждены отвлекать машины скорой медицинской помощи, отменять приемы и откладывать оказание помощи, перевозить пациентов в другие больницы. Многие посягательства привели к сбоям в работе на несколько месяцев, а некоторые нападения привели к окончательному закрытию медицинских учреждений. Сосредоточив внимание на передовых протоколах безопасности, обнаружении уязвимостей и автоматических исправлениях, усилия должны быть направлены на уменьшение возможностей злоумышленников атаковать программное обеспечение цифрового здравоохранения, что в целом позволит предотвратить крупномасштабные кибератаки.

Основными элементами цифровой безопасности системы здравоохранения являются:

- безопасность цифровой информации, обращающейся в учреждениях системы здравоохранения;
- безопасность цифровой инфраструктуры учреждений системы здравоохранения;
- безопасность цифровых технологий, используемых в учреждениях системы здравоохранения различного уровня.

Заключение. Во-первых, цифровые технологии, применяемые в сфере здравоохранения, активно применяются уже сейчас и имеют огромные перспективы в целях охраны здоровья граждан;

во-вторых, в результате цифровизации на учреждения системы здравоохранения будут совершаться противоправные посягательства, следовательно, необходимо принимать меры по их уголовно-правовой охране;

в-третьих, имеются риски совершения противоправных посягательств в цифровой среде в отношении национальных систем здравоохранения, в том числе нападения на объекты военной медицины, которые уже составляют угрозу национальной безопасности Российской Федерации в целом;

в-четвертых, именно средства уголовного права как наиболее карательной отрасли с точки зрения применяемых санкций должны быть направлены на криминальные угрозы цифровой безопасности системы здравоохранения.

В результате исследования нами был сформирован понятийно-категориальный аппарат, который, по нашему мнению, расширит отечественную науку

и может быть использован при совершенствовании действующего законодательства:

Здравоохранение – сфера общественной жизни, одно из направлений государства, область правоотношений, возникаемых в связи с реализацией конституционного принципа охраны здоровья каждого человека и оказания ему медицинской помощи.

Цифровое здравоохранение – это широкая междисциплинарная концепция, возникшая на стыке цифровых технологий и здравоохранения, представляющая под собой область знаний и практики, связанную с созданием (разработкой) и применением цифровых технологий, а также средств и методов ее обеспечения (цифровой информации и цифровой инфраструктуры) в учреждениях системы здравоохранения.

Цифровая безопасность системы здравоохранения – состояние защищенности цифровой информации, цифровой инфраструктуры и цифровых технологий в системе здравоохранения от внутренних и внешних цифровых угроз.

Цифровая угроза – совокупность условий и факторов, направленных на нарушение безопасности цифровой информации, цифровой инфраструктуры и цифровых технологий.

Обеспечение цифровой безопасности системы здравоохранения – деятельность по защите цифровой информации, цифровой инфраструктуры и цифровых технологий от цифровых угроз путем обеспечения правовым, организационно-техническим и иным мероприятиям по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению угроз и ликвидации их последствий.

Список литературы

1. Ненашева Е. А. Обзор медицинского программного обеспечения с искусственным интеллектом // Наука и образование сегодня. 2019. № 9 (44). С. 27–30.
2. Stoumpos A. I., Kitsios F., Talias M. A. Digital Transformation in Healthcare: Technology Acceptance and Its Applications. *Int J Environ Res Public Health*. 2023 Feb 15;20(4):3407. doi: 10.3390/ijerph20043407. PMID: 36834105; PMCID: PMC9963556.
3. Verga M., Viganò G. L., Capuzzo M., Duri C., Ignotti L. M., Picozzi P., Cimolin V. The digitization process and the evolution of Clinical Risk Management concept: The role of Clinical Engineering in the operational management of biomedical technologies. *Front Public Health*. 2023 Feb 2;11:1121243. doi: 10.3389/fpubh.2023.1121243. PMID: 36817927; PMCID: PMC9932586.
4. Распоряжение Правительства Российской Федерации от 29 декабря 2021 г. № 3980-р // Собрание законодательства Российской Федерации. 2022. № 1 (ч. IV), ст. 434.
5. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента Российской Федерации от 7 мая 2018 г. № 204 // Собрание законодательства Российской Федерации. 2018. № 20, ст. 2817.
6. О Стратегии развития здравоохранения в Российской Федерации на период до 2025 года: Указ Президента Российской Федерации от 6 июня 2019 г.

№ 254 // Собрание законодательства Российской Федерации. 2019. № 23, ст. 2927.

7. О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 21 июля 2020 г. № 474 // Собрание законодательства Российской Федерации. 2020. № 30, ст. 4884.

8. Об утверждении государственной программы Российской Федерации «Развитие здравоохранения: постановление Правительства Российской Федерации от 26 декабря 2017 г. № 1640 // Собрание законодательства Российской Федерации. 2018. № 1 (ч. II), ст. 373.

9. Маркина А. Ю., Посулихина Н. С. Краткий очерк цифровизации медицины // Вестник Университета имени О. Е. Кутафина. 2023. №. 6 (106). С. 124–131.

10. Карпов О. Э., Субботин С. А., Шишканов Д. В., Замятин М. Н. Цифровое здравоохранение. Необходимость и предпосылки // Врач и информационные технологии. 2017. №. 3. С. 6-22.

11. Владимир Путин попросил ускорить принятие проекта программы цифровизации здравоохранения: [сайт]. URL: <https://d-russia.ru/vladimir-putin-poprosil-uskorit-prinyatie-proekta-programmy-tsifrovizatsii-zdravooohraneniya.html> (дата обращения: 11.09.2024).

12. Карцхия А. А. Цифровая медицина – реальность сегодняшнего дня // Экономические и социальные проблемы России. 2021. № 2 (46). С. 132-142.

13. Гараева А. С., Залоило М. В., Полещук И. А., Власова Н. В., Гераськина Н. С. Исторические предпосылки внедрения телемедицинских технологий в сферу здравоохранения в России // Вопросы истории. 2020. № 12(1). С. 218–225.

14. Гараева А. С., Залоило М. В., Полещук И. А., Власова Н. В., Фомина Е. В. Телемедицина в России: опыт осмысления в юридической доктрине и становление правового регулирования // Вопросы истории. 2020. № 11(1). С. 243–248.

15. Об утверждении государственной программы Российской Федерации «Развитие здравоохранения, Концепция информационной безопасности в сфере здравоохранения» (приложение № 2 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 10 марта 2022 г. № 7): Постановление Правительства Российской Федерации от 26 декабря 2017 г. № 1640 // Собрание законодательства Российской Федерации. 2018. № 1 (ч. II), ст. 373.

16. Проект глобальной стратегии в области цифрового здравоохранения на 2020–2025 гг.: [сайт]. URL: <https://www.who.int/docs/default-source/documents/200067-draft-global-strategy-on-digital-health-2020-2024-ru.pdf> (дата обращения: 01.09.2024).

17. United States Food and Drug Administration. 2018. Digital Health: [сайт]. URL: <https://www.fda.gov/medicaldevices/digitalhealth/> [accessed 2018-06-07] [WebCite Cache] (дата обращения: 21.08.2024).

18. Об утверждении Разъяснений (методических рекомендаций) по разработке региональных проектов в рамках федеральных проектов национальной программы «Цифровая экономика Российской Федерации: Приказ Минкомсвязи России от 1 августа 2018 г. № 428 // СПС «КонсультантПлюс».

19. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. 2017. № 20, ст. 2901.
20. Коданева С. И. Цифровые технологии в здравоохранении: зарубежный опыт // Россия: тенденции и перспективы развития. 2020. № 15-1. С. 617–620.
21. Карцхия А. А. Формирование параметров здравоохранения как вызов времени // Право и цифровая экономика. 2021. № 3 (13). С. 39–46.
22. G. L. Tortorella, T. A. Saurin, F. S. Fogliatto, V. M. Rosa, L. M. Tonetto, F. Magrabi. Impacts of Healthcare 4.0 digital technologies on the resilience of hospitals Technol. Forecast. Soc. Change, 166 (2021), Article 120666 <https://doi.org/https://doi.org/10.1016/j.techfore.2021.120666>
23. G. Aceto, V. Persico, A. Pescapé. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges J. Netw. Comput. Appl., 107 (2018), pp. 125–154.
24. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. Healthcare Data Breaches: Insights and Implications. Healthcare (Basel). 2020 May 13;8(2):133. doi: 10.3390/healthcare8020133.
25. Argaw ST, Troncoso-Pastoriza J, Lacey D, Florin M, Calcavecchia F, Anderson D, Burleson W, Vogel JM, O'Leary C, Eshaya-Chauvin B, Flahault A. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak. 2020 Jul 03;20(1):146. doi: 10.1186/s12911-020-01161-7.
26. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. J King Saud Univ Comput Inf Sci. 2022 Nov;34(10):8176-8206. doi: 10.1016/j.jksuci.2022.08.003.
27. Шутова А. А. Угрозы информационной безопасности учреждений системы здравоохранения: уголовно-правовой аспект // Вестник Уфимского юридического института МВД России. 2023. № 3(101). С. 131–137. EDN BQZHXU.
28. Рускевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650–672. EDN FISEET.
29. Гончаров И. В. О соотношении понятий «Национальная безопасность», «Государственная безопасность», «Конституционная безопасность» // Актуальные проблемы российского права. 2009. № 1. С. 116–122.
30. О безопасности: Закон Российской Федерации от 5 марта 1992 г. № 2446-I // Российская газета. 1992, 6 мая (утратил силу).
31. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации. 2021. № 27 (ч. II), ст. 5351.
32. О безопасности дорожного движения: Федеральный закон от 10 декабря 1995 г. № 196-ФЗ // Собрание законодательства Российской Федерации. 1995. № 50, ст. 4873.

МУЛЬТИДИСЦИПЛИНАРНЫЕ (НЕЮРИДИЧЕСКИЕ) АСПЕКТЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

В.-М. Д. Аникеева,

студент,

Волгоградский государственный аграрный университет

О. В. Кочеткова,

доктор технических наук, профессор

Волгоградский государственный аграрный университет

ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ РАЗРАБОТКИ ЭКСПЕРТНОЙ СИСТЕМЫ ПО ПОДДЕРЖКЕ ПРИНЯТИЯ РЕШЕНИЙ ПО ПЕРЕВОДУ ГОСУДАРСТВЕННЫХ УСЛУГ В ЭЛЕКТРОННУЮ ФОРМУ ПРЕДСТАВЛЕНИЯ

Аннотация. Единый портал государственных и муниципальных услуг (ЕПГУ) – государственная информационная система, обеспечивающая предоставление государственных и муниципальных услуг в электронной форме. ЕПГУ имеет большой потенциал развития в части увеличения количества государственных услуг доступных в электронном виде, но процесс перевода государственных услуг в электронную форму имеет большое количество вариантов реализации. Целью данной работы является обоснование целесообразности разработки экспертной системы для поддержки принятия решений по переводу государственных услуг в электронную форму предоставления.

Ключевые слова: информационные технологии, экспертная система, государственные услуги, поддержка принятия решения, Единый портал государственных и муниципальных услуг, архитектура процесса принятия решения, обоснование необходимости разработки

JUSTIFICATION OF THE EXPEDIENCY OF DEVELOPING AN EXPERT SYSTEM TO SUPPORT DECISION-MAKING ON THE TRANSFER OF PUBLIC SERVICES TO AN ELECTRONIC FORM OF PROVISION

Abstract. The Unified Portal of State and Municipal Services (EPSU) is a state information system that provides state and municipal services in electronic form. The EPSU has great development potential in terms of increasing the number of public services available in electronic form, but the process of converting public services into electronic form has a large number of implementation options. The purpose of this work is to substantiate the feasibility of developing an expert system to support decision-making on the transfer of public services to an electronic form of provision.

Keywords: information technology, expert system, public services, decision support, Unified portal of state and municipal services, architecture of the decision-making process, justification of the need for development

Введение. В настоящее время Интернет – наиболее дешевый канал взаимодействия с населением – открывает широкие возможности для самообслуживания. Активное развитие Интернета привело к смещению акцента с концепции государственных услуг к электронным государственным услугам [1].

Единый портал государственных и муниципальных услуг (ЕПГУ) – государственная информационная система, обеспечивающая предоставление государственных и муниципальных услуг в электронной форме, а также доступ заявителей к сведениям о государственных и муниципальных услугах, предназначенным для распространения с использованием информационно-телекоммуникационной сети «Интернет» и размещенным в государственных и муниципальных информационных системах, обеспечивающих ведение реестров государственных и муниципальных услуг [5].

Основной целью внедрения электронной формы предоставления государственных услуг является стандартизация путем выявления и формализации через регламенты оказания. Это позволяет фиксировать качество сервиса и последовательно работать над его повышением. Также внедрение технологий самообслуживания помогает в снижении стоимости оказания услуги и уменьшении коррупционной составляющей при оказании услуг за счет устранения личного взаимодействия заявителей с государственными служащими.

Основная часть. Государственные услуги, предоставляемые в электронной форме посредством ЕПГУ, позволяют оформлять документы, получать пособия и страховые возмещения, следить за исполнительными производствами и даже поступать в вуз без личного визита, очередей и бумажных бланков [7].

Популярность ЕПГУ среди населения стремительно растет. По информации оператора ЕПГУ – Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, число пользователей ЕПГУ с 2019 года увеличилось в два раза, к концу 2023 года составило 109 млн человек (75% от населения Российской Федерации). За 2023 год прирост составил 10,2 млн человек [13].

В соответствии с указом Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» от 07.05.2024 № 309 установлена задача увеличения к 2030 году до 99% доли предоставления массовых социально значимых государственных и муниципальных услуг в электронной форме [12].

Перевод государственных услуг в электронную форму предоставления является важным шагом к построению информационного общества, повышению качества оказываемых органами власти услуг, росту доверия со стороны населения и минимизации коррупционной составляющей в процессе оказания государственных и муниципальных услуг [11].

ЕПГУ имеет большой потенциал развития в части увеличения количества государственных услуг доступных в электронном виде, но процесс перевода

государственных услуг в электронную форму имеет большое количество вариантов реализации.

Проблема исследования заключается в слабой формализации процесса принятия решения и большого количества слабоструктурированных данных, необходимых для принятия решения. Для принятия решения использования одного из вариантов перевода государственных услуг в электронную форму нужны квалифицированные специалисты, которых не хватает в данной отрасли. Поэтому появляется необходимость в разработке экспертной системы.

Гипотеза: экспертная система поможет принимать решения по переводу государственных услуг в электронную форму предоставления. Это позволит сократить время, затрачиваемое на принятие решений, а также снизить количество ошибок. Гипотеза достижима, потому как не требует больших затрат ресурсов. В данной предметной области имеются квалифицированные специалисты и эксперты.

Целью данного исследования является обоснование целесообразности разработки экспертной системы для поддержки принятия решений по переводу государственных услуг в электронную форму предоставления.

Выбор объекта исследования и сбор материалов об объекте исследования. Рассмотрим схему взаимодействия заявителя и сотрудника ведомства, предоставляющего государственные или муниципальные услуги (рис. 1). Заявитель посредством интерактивной формы, расположенной на Едином портале государственных и муниципальных услуг, подает заявление на предоставление услуги. Заявление через Систему межведомственного электронного взаимодействия попадает в ведомственную информационную систему, в которой заявление обрабатывает сотрудник ведомства. Результат предоставления услуги попадает к заявителю в личный кабинет на Едином портале государственных и муниципальных услуг.

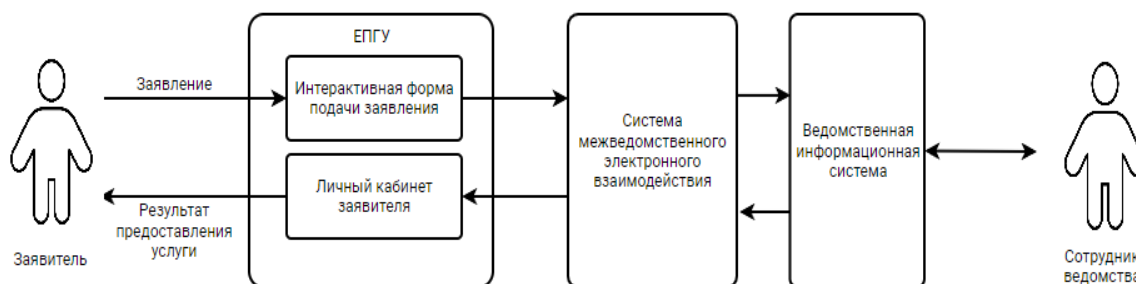


Рис. 1. Схема взаимодействия заявителя и сотрудника ведомства

Объектом исследования является процесс принятия решений по переводу государственных услуг в электронную форму предоставления.

Рассмотрим все возможные варианты реализации перевода государственных и муниципальных услуг в электронную форму предоставления на Едином портале государственных и муниципальных услуг в зависимости от факторов, влияющих на принятие решения.

Интерактивную форму для подачи заявления разрабатывают сотрудники федеральных ведомств, сотрудники региональных ведомств или подрядные организации.

В случае если интерактивная форма разработана федеральным ведомством, региональные ведомства могут подключиться к ней без затрат своих ресурсов. Только среди региональных услуг выделено 243 типовых услуги, для которых может быть разработана единая федеральная форма. Перечень таких услуг постоянно дополняется [9].

Если федеральное ведомство не разработало единую для всех регионов интерактивную форму, региональные ведомства могут разработать ее сами силами своих сотрудников или с привлечением подрядных организаций. В этом случае затрачивается большое количество ресурсов и времени.

Возможен вариант, когда разработанная интерактивная форма не используется в регионе по причине наличия доказанной региональной специфики услуги, тогда можно на основе уже разработанной формы создать новую.

В случае необходимости разработки новой региональной формы необходимо учитывать востребованность услуги среди заявителей, актуальность услуги, наличие согласования Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации перевода услуги в электронную форму, сложность разработки интерактивной формы и соответствие нормативно правовых актов требованиям.

Услуга может быть очень востребована среди населения, такие услуги переводят в электронный вид в первую очередь. Если услуга не очень востребована, но имеет минимум два заявления в год, то ее можно переводить в электронный вид при необходимости. Если за предоставлением услуги обращаются менее двух раз в год, то услуга считается невостребованной среди населения и разработка электронной формы для нее нецелесообразна.

Необходимо учитывать актуальность услуги. Если услугу прекратят предоставлять в ближайшее время или передадут полномочия на ее предоставление на федеральный уровень, то разработка электронной формы для нее нецелесообразна.

Для вывода на Единый портал государственных и муниципальных услуг интерактивной формы услуги необходимо согласование уполномоченного органа – Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Для этого перед разработкой интерактивной формы в Минцифры на согласование направляется информация об услуге. Минцифры может согласовать разработку интерактивной формы, согласовать с замечаниями или не согласовать [8].

Если разработка согласована при условии устранения замечаний, то перед разработкой интерактивной формы ведомство, ответственное за предоставление услуги должно устранить замечания. Если разработка не согласована, то дальнейшие действия зависят от причин несогласования. Разработка откладывается на следующий год, потребуется повторно отправить информацию об услуге в Минцифры.

От сложности разработки интерактивной формы зависит стоимость разработки. В рамках одной услуги могут предоставляться несколько подуслуг, что

незначительно усложняет процесс разработки. Необходимость подписания документов в ходе предоставления услуги в мобильном приложении «Госключ» или потребность в онлайн-записи на прием в ведомство требует покупки дополнительных модулей для ведомственных информационных систем. Если использование интерактивной формы планируется в нескольких ведомствах, потребуется создание дополнительных справочников, что усложняет процесс разработки.

Стоит учитывать сложность процесса предоставления услуги. Если услуга предоставляется в один этап, без необходимости прикрепления заявителем дополнительных документов (например, получение различных выписок), то разработка считается простой и имеет низкую стоимость.

Перед принятием решения по разработке формы необходимо учитывать актуальность административного регламента предоставления услуги. Если регламент устарел, то ведомство может его актуализировать после разработки формы, соответственно форма потеряет свою актуальность или Минцифры не согласует вывод интерактивной формы, разработанной в соответствии с устаревшим регламентом. Также Минцифры не согласует вывод интерактивной формы услуги, если в административном регламенте предоставления услуги не закреплен способ подачи заявления через Единый портал государственных и муниципальных услуг [8].

Если услуга является муниципальной, для нее обязательно должен быть разработан и утвержден единый модельный административный регламент. Иначе разработка формы представляется нереализуемой.

Также необходимо учитывать специфику услуги в части сферы ее предоставления. От сферы предоставления зависит, какую ведомственную информационную систему нужно использовать для обработки заявлений поступающих с Единого портала государственных и муниципальных услуг.

В настоящее время используются следующие ведомственные информационные системы:

федерального уровня:

- платформа государственных сервисов;
- типовое облачное решение контрольной (надзорной) деятельности;
- единая автоматизированная информационная система «Росздравнадзора».

регионального уровня:

- автоматизированное рабочее место «Модуль оказания услуг»;
- государственная информационная система обеспечения градостроительной деятельности;
- государственная информационная система «Охотучет»;
- государственная информационная система учета и регистрации тракторов, самоходных машин и прицепов к ним;
- катарсис: соцзащита;
- государственная информационная система «Образование Волгоградской области».

Для наглядности далее представлена когнитивная карта всех факторов, учитываемых при принятии решения по переводу государственных услуг в электронную форму предоставления (рис. 2).

Данный процесс занимает большое количество времени и приводит к ошибочно принятым решениям, что, в свою очередь, ведет к стоимостным и репутационным рискам. Необходимо разработать более рациональную стратегию принятия решения по переводу государственных услуг в электронную форму.

Обоснование научной новизны исследования. Ранее мы определили, что существующий алгоритм принятия решения по переводу государственных услуг в электронную форму занимает большое количество времени и приводит к ошибочно принятым решениям, что в свою очередь ведет к стоимостным и репутационным рискам. Необходимо разработать более рациональную стратегию принятия решения по переводу государственных услуг в электронную форму.

В настоящее время не существует четко формализованного процесса принятия решения, учитывающего все влияющие факторы. Например, Рязанов Яков Николаевич, студент магистратуры Тюменского государственного университета, описывает процесс перевода государственных и муниципальных услуг в электронный в несколько этапов. Во-первых, должна быть оценена правовая основа перевода государственной услуги в электронный вид, а также, при необходимости, внесение в законодательство изменений в установленном порядке. После оценивается социальная и экономическая эффективность перевода государственной услуги в электронный вид, выявление возможных рисков и наличия технической возможности реализации услуги в электронном виде, изучается передовой опыт предоставления аналогичных услуг в электронном виде не только в других регионах России, но и зарубежный опыт. Подготавливается техническая документация и создается узкоспециализированное программное обеспечение. Производится тестирование и отладка сервиса (в этот этап, как правило, включают этап обучения специалистов регистрирующих органов, которые будут предоставлять эти услуги). Определяется пилотная зона эксплуатации сервиса. Лишь после всего этого осуществляется ввод в эксплуатацию сервиса [10].

Данный алгоритм не учитывает все необходимые факторы, выявленные нами ранее и также занимает большое количество времени. Все остальные найденные исследования не отражают процесс принятия решений по переводу государственных услуг в электронную форму предоставления.

Также стоит отметить, что в 2023 году была изменена архитектура ЕПГУ и полностью изменился порядок разработки и размещения на ЕПГУ интерактивных форм услуг. Теперь интерактивная форма заявления разрабатывается только с использованием подсистемы ЕПГУ Визуального конструктора услуг, предоставляющей функциональные механизмы интерактивной среды разработки, хранения и тестирования разрабатываемых интерактивных форм заявлений [8].

Приказом Минцифры России от 10.07.2023 № 625 были выведены из эксплуатации все разработанные ранее интерактивные формы сообщений, обращений и заявлений. Отключены разделы «Категории услуг», «Органы власти» и др.

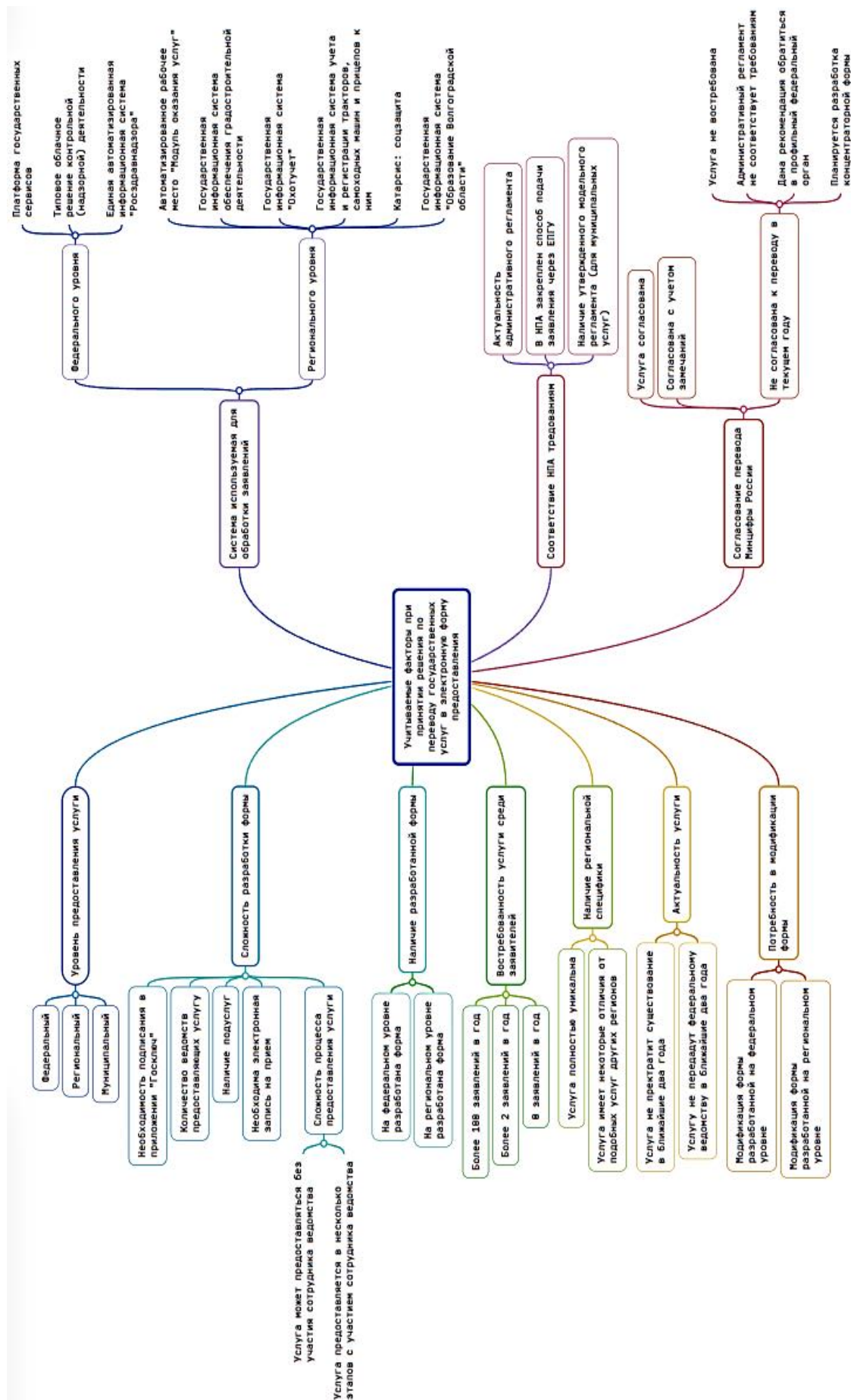


Рис. 2. Когнитивная карта факторов, учитываемых при принятии решения по переводу государственных услуг в электронную форму предоставления

В связи с изменением архитектуры ЕПГУ и порядком разработки и размещения на ЕПГУ интерактивных форм услуг, исследования проведенные в сфере перевода государственных услуг в электронную форму предоставления посредством ЕПГУ неприменимы к настоящей архитектуре ЕПГУ и процессу вывода на него интерактивных форм услуг.

В данной работе планируется впервые представить новый алгоритм принятия решений, позволяющий осуществлять выбор наилучшего способа перевода государственных услуг в электронную форму предоставления и учитывающий все факторы, влияющие на принятие решения.

В настоящее время весь процесс принятия решения по переводу в электронную форму государственной услуги производится аналитиком вручную (рис. 3). Аналитик собирает все возможные данные об услуге, даже те данные, которые могут не понадобиться при принятии решения. Далее поочередно рассматриваются все возможные факторы, влияющие на принятие решения. Затем из всех рассмотренных факторов выявляются те, которые оказывают влияние на принятие решения в отношении конкретной услуги, и принимается окончательное решение по переводу государственной услуги в электронную форму.



Рис. 3. eEPC диаграмма процесса принятия решения по переводу государственной услуги в электронную форму

Далее представлен процесс принятия решения по переводу государственной услуги в электронную форму с использованием экспертной системы (рис. 4). Теперь аналитик собирает только необходимые данные об услуге и затем принимает решение с помощью экспертной системы. Новый алгоритм принятия решений, используемый в экспертной системе, позволяет исключить процессы поочередного рассмотрения всех возможных факторов влияющих на принятие ре-

шения и выявления факторов, оказывающих влияние на принятие решения в отношении конкретной услуги, так как алгоритм будет рассматривать только факторы оказывающие влияние на конкретную услугу и не будет рассматривать все возможные факторы поочередно, до тех пор пока не будет принято решение. Это значительно сократит время принятия решения и количество ошибочно принятых решений.



Рис. 4. eEPC диаграмма процесса принятия решения по переводу государственной услуги в электронную форму с использованием экспертной системы

Изучение архитектуры процесса принятия решения по переводу государственных услуг в электронную форму и обоснование необходимости разработки экспертной системы. Процесс принятия решений по переводу государственных услуг в электронную форму предоставления будет изучен более детально на примере работы центра компетенции автоматизации предоставления государственных и муниципальных услуг государственного бюджетного учреждения Волгоградской области «Центр информационных технологий Волгоградской области».

Центр – подразделение, предназначенное для обеспечения процедур и координации работ, проводимых органами исполнительной власти Волгоградской области в целях перевода в электронную форму государственных и муниципальных услуг Волгоградской области, анализа подлежащих автоматизации бизнес процессов органов власти, обеспечения доступа к региональным информационным ресурсам, обеспечивающим процесс государственных и муниципальных услуг Волгоградской области в электронной форме.

Опишем существующую бизнес-архитектуру. В существующей архитектуре бизнес-роль «Аналитик» назначена на выполнение бизнес-функционала «Принятие решения по переводу государственных услуг в электронную форму предоставления». Бизнес-функционал «Принятие решения по переводу государственных услуг в электронную форму предоставления» назначен на процессы сбора всех возможных данных об услуге, рассмотрения возможных факторов влияющих на принятие решения, выявления факторов влияющих на принятие решения в отношении конкретной услуги, принятия решения по переводу госу-

дарственной услуги в электронную форму и составления отчета о принятом решении. В результате процесса составления отчета о принятом решении получаем бизнес-объект «Отчет», к которому имеет доступ бизнес-функционал «Направление отчета» назначенный бизнес-роли «Начальник ЦК АГМУ».

Опишем слой приложений существующей архитектуры. Процессы сбора всех возможных данных об услуге, рассмотрения возможных факторов, влияющих на принятие решения, выявления факторов, влияющих на принятие решения в отношении конкретной услуги, принятия решения по переводу государственной услуги в электронную форму производятся:

- посредством сервиса поиска и сервиса работы с данными на Едином портале государственных и муниципальных услуг через интерфейс ЕПГУ;
- посредством сервиса работы с документами Автоматизированной системы электронного документооборота через интерфейс АСЭД;
- посредством сервиса работы с документами справочной правовой системы КонсультантПлюс через интерфейс КонсультантПлюс.

Компонент приложений «Продукты Microsoft Office», состоящий из текстового редактора и редактора таблиц, реализует сервис работы с документами и сервис работы с электронными таблицами, эти сервисы доступны через интерфейс продуктов Microsoft, через него аналитик реализует все процессы бизнес-функционала «Принятие решения по переводу государственных услуг в электронную форму предоставления».

Опишем существующую технологическую архитектуру. Узел «Федеральный центр обработки данных» реализует инфраструктурный функционал обработки данных и хранения данных. Данный функционал реализуется через сервис обработки данных и сервис хранения данных. Эти сервисы использует Единый портал государственных и муниципальных услуг. Устройством «ПК сотрудника» реализуется инфраструктурный функционал обработки и хранения данных. Данный функционал реализуется через сервис обработки данных и сервис хранения данных. Эти сервисы используются Продуктами Microsoft Office, Автоматизированной системой электронного документооборота, справочной правовой системой КонсультантПлюс. ПК сотрудника и Федеральный центр обработки данных соединены коммуникационным соединением. Верхнеуровневая модель существующей архитектуры процесса принятия решения по переводу государственных услуг в электронную форму предоставления в нотации ArchiMate представлена далее (рис. 5).

На данной модели видно, что аналитик вручную производит рассмотрение всех возможных факторов, влияющих на принятие решения, выявление факторов, влияющих на принятие решения в отношении конкретной услуги, а также принятие решения по переводу государственной услуги в электронную форму и составление отчета о принятом решении. Процессы сбора всех возможных данных об услуге и рассмотрения всех возможных факторов занимают больше всего времени и производятся посредством поиска информации на Едином портале государственных и муниципальных услуг, в официальных документах, содержащихся в автоматизированной системе электронного документооборота, в нормативно-правовых актах в справочной системе «КонсультантПлюс», в электронных таблицах, собранных ранее.

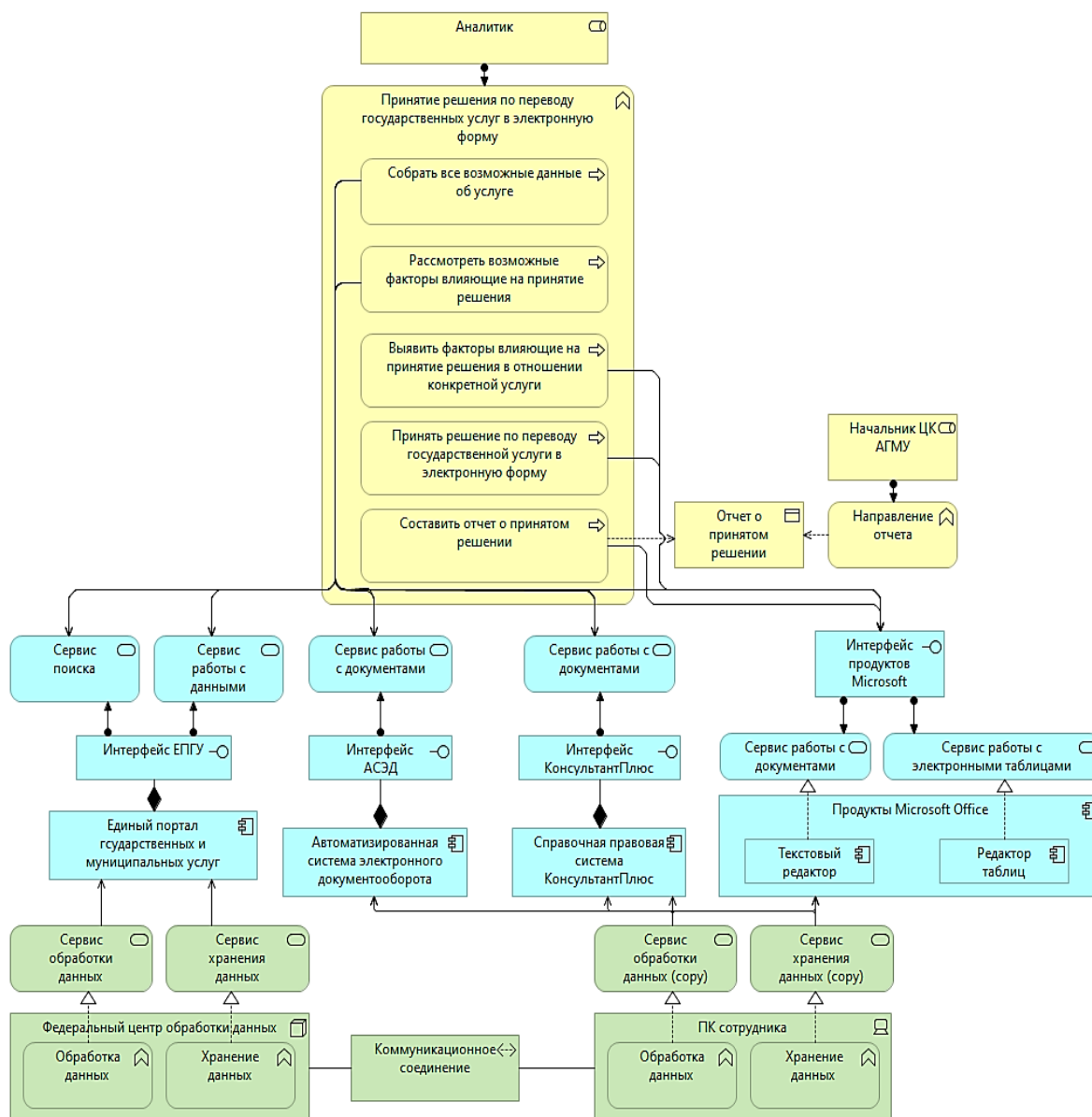


Рис. 5. Верхнеуровневая модель существующей архитектуры процесса принятия решения по переводу государственных услуг в электронную форму предоставления

Посредством разработки экспертной системы можно автоматизировать процессы рассмотрения возможных факторов, влияющих на принятие решения, выявления факторов, влияющих на принятие решения в отношении конкретной услуги, принятия решения по переводу государственной услуги в электронную форму и составления отчета о принятом решении.

Автоматизация данных процессов посредством разработки экспертной системы позволит ускорить процесс принятия решения и сократить количество ошибочных решений.

Начальник ЦК АГМУ мотивирован оптимальностью процесса принятия решения (рис. 6). Имеется такие оценки, как «процесс принятия решения происходит медленно» и «принимается большое количество ошибочных решений». Для достижения цели работы «улучшить процесс принятия решения» необходимо ускорить процесс принятия решения и сократить количество ошибочных решений. Данные задачи решаются путем обеспечения сервиса автоматизированной консультации посредством разработки экспертной системы.

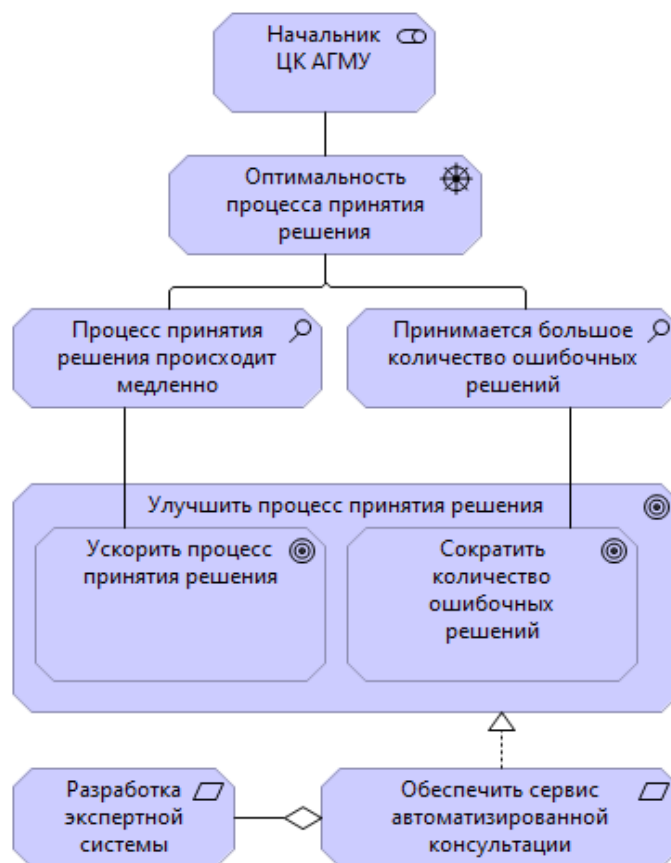


Рис. 6. Модель мотивации

Необходимо обеспечить сервис автоматизированной консультации пользователя посредством разработки экспертной системы. Разработанная экспертная система по поддержке принятия решения по переводу государственных услуг в электронную форму предоставления будет осуществлять процессы выявления факторов, влияющих на принятие решения в отношении конкретной услуги, принятия решения по переводу государственной услуги в электронную форму и составление отчета о принятом решении (рис. 7). Экспертная система реализует сервис консультации пользователя, которому назначен интерфейс экспертной системы. Интерфейс экспертной системы используется новым процессом проведения консультации с экспертной системой. Процесс составления отчета о принятом решении создает объект данных «Отчет о принятом решении», который потом направляется начальнику ЦК АГМУ.

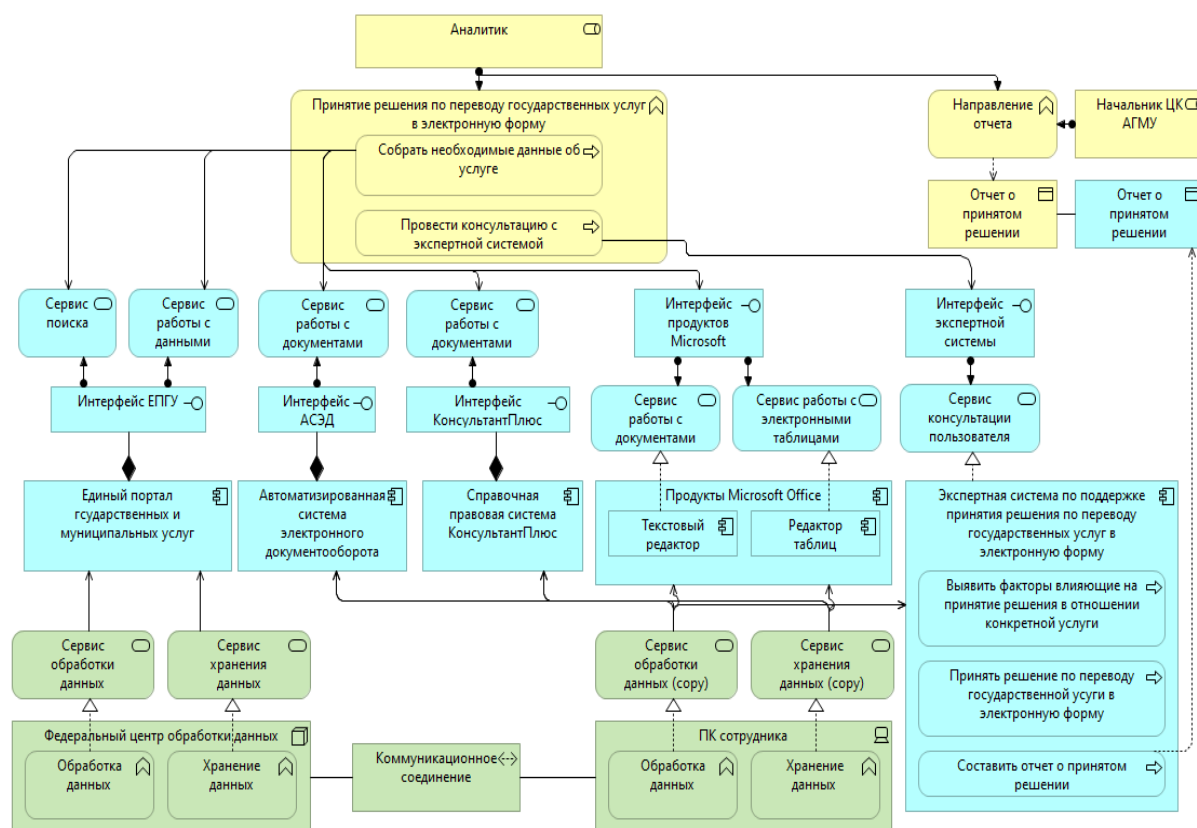


Рис. 7. Модель целевой архитектуры процесса принятия решения по переводу государственных услуг в электронную форму предоставления

Таким образом, с помощью экспертной системы автоматизированы процессы выявления факторов, влияющих на принятие решения в отношении конкретной услуги, принятия решения по переводу государственной услуги в электронную форму и составления отчета о принятом решении.

Новый алгоритм принятия решений, позволяющий осуществлять выбор наилучшего способа перевода государственных услуг в электронную форму предоставления, используемый экспертной системой, позволяет исключить процесс рассмотрения всех возможных факторов, влияющих на принятие решения. Алгоритм сразу будет выявлять факторы, влияющие на принятие решения в отношении конкретной услуги.

Также процесс сбора всех возможных данных об услуге заменен на процесс сбора только необходимых данных об услуге. Так как экспертная система позволяет не рассматривать все возможные факторы, влияющие на принятие решения, то и данные об услуге понадобятся не все возможные, а только необходимые.

Практическую значимость работы составляет улучшение процессов принятия решений по переводу государственных услуг в электронную форму предоставления в центре компетенции автоматизации предоставления государственных и муниципальных услуг государственного бюджетного учреждения

Волгоградской области «Центр информационных технологий Волгоградской области».

Оправданность использования экспертной системы. Разработка экспертной системы возможна по следующим причинам [2]:

- в области перевода государственных и муниципальных услуг существуют квалифицированные эксперты;
- эксперты сходятся в оценке предлагаемого решения, что означает возможность оценки качества разработанной экспертной системы;
- знания экспертов легко внести в экспертную систему, так как эксперты способны объяснить используемые ими методы;
- решение задачи требует только рассуждений, а не действий;
- задача является узконаправленной;
- решение задачи не использует абстрактное мышление.

Использование экспертной системы в области перевода государственных и муниципальных услуг оправдано, так как присутствуют следующие факторы [2]: использование услуг эксперта не всегда реализуемо, так как опытных специалистов в области перевода государственных услуг в электронную форму предоставления недостаточное количество; процесс принятия решения слабо формализован и требует анализа большого количества слабо структурированных данных.

Созданное приложение соответствует методам ЭС, так как решаемая задача обладает совокупностью следующих характеристик [2]: она может быть решена естественным образом с помощью символических рассуждений; имеет эвристическую природу; достаточно сложна, что оправдывает затраты на разработку экспертной системы, но не сложна настолько чтобы экспертная система не могла с ней справиться; является достаточно узконаправленной и практически значимой.

Постановка целей и задач разработки экспертной системы. Целью разработки экспертной системы является снижение количества неверно принятых решений, сокращение времени выявления нужного решения.

Задачи разработки экспертной системы: изучить основные проектные решения экспертных систем; разработать стратегию принятия решения; выбрать инструментарий для разработки экспертной системы; создать правила для экспертной системы.

Разработка требований к экспертной системе. Экспертная система разрабатывается для улучшения процессов принятия решений по переводу государственных услуг в электронную форму предоставления в центре компетенции автоматизации предоставления государственных и муниципальных услуг государственного бюджетного учреждения Волгоградской области «Центр информационных технологий Волгоградской области».

Заказчиком ГБУ ВО «ЦИТ ВО» были сформулированы требования к экспертной системе: она должна обеспечивать возможность модификации алгоритма принятия решения при обновлении информации; иметь возможность быстрого принятия решения; предлагать возможные варианты решения проблемных вопросов, возникающих в ходе консультации, и наилучшее подходящее решение.

Заключение. В результате проведения настоящей работы обоснована целесообразность разработки экспертной системы для поддержки принятия решений по переводу государственных услуг в электронную форму предоставления.

Для этого были решены следующие задачи:

- проведен анализ предметной области;
- изучена архитектура процесса принятия решения по переводу государственных услуг в электронную форму и обоснование необходимости разработки экспертной системы;
- обоснована научная новизна исследования;
- доказана оправданность использования экспертной системы;
- поставлена цель и задачи разработки экспертной системы;
- разработаны требования к экспертной системе.

Установлено, что разработка запросов к экспертной системе в соответствии с составленной картой факторов, учитываемых при принятии решения по переводу государственных услуг в электронную форму предоставления не является рациональной, поскольку такой алгоритм занимает большое количество времени и приводит к ошибочно принятым решениям, что в свою очередь ведет к стоимостным и репутационным рискам.

Необходимо разработать более рациональную стратегию принятия решения по переводу государственных услуг в электронную форму.

Список литературы

1. Ализаде М. Г. Государственные услуги в России: понятие и виды // Вестник Университета имени О. Е. Кутафина. – 2019. – №6. – С. 174–178.
2. Бердышев А. С., Калиева К. А., Кантуреева М. А. О методологии проектирования экспертных систем // Проблемы информатики. – 2013. – № 1 (18).
3. Государственное бюджетное учреждение Волгоградской области «Центр информационных технологий» [Электронный ресурс] // URL: <https://citvo.ru> (дата обращения: 03.03.2023).
4. Грекул В. И., Коровкина Н. Л., Левочкина Г. А. Проектирование информационных систем: учебник и практикум для вузов. – М.: Юрайт, 2020. – 385 с.
5. Закон Российской Федерации «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ // Собрание законодательства Российской Федерации. – 2010. – № 31. – Ст. 2.
6. Зараменских Е. П., Кудрявцев Д. В., Арзуманян М. Ю. Архитектура предприятия: учебник для вузов / под ред. Е. П. Зараменских. – М.: Юрайт, 2020. – 410 с.
7. Ильгуватова А. И. Портал государственных услуг Российской Федерации // Научный электронный журнал «Профессиональное образование Арктических регионов», 2020. – № 3. – С. 11– 13.
8. Постановление Правительства Российской Федерации «Об утверждении Правил разработки и размещения в федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)» интерактивных форм сообщений, обращений, заявлений и документов, а также заявлений об электронной записи на прием» от 03.09.2022 № 1555 // Собрание законодательства РФ. – 2022. – № 37.

9. Распоряжение Правительства Российской Федерации «О Перечне типовых государственных и муниципальных услуг, предоставляемых исполнительными органами субъектов Российской Федерации, государственными учреждениями субъектов Российской Федерации и муниципальными учреждениями, а также органами местного самоуправления» от 18.09.2019 № 2113-р // Собрание законодательства РФ. – 2019. – № 39.

10. Рязанов Я. Н. Предоставление государственных и муниципальных услуг в электронной форме: проблемы и пути решения // Молодой ученый. – 2019. – № 26 (264). – С. 238–240.

11. Толкачев М. В. Правовые основы перевода оказания государственных услуг в электронный вид на примере города Москвы // Аграрное и земельное право [Электронный ресурс]. – 2023. – №8. – URL: <https://cyberleninka.ru/article/n/pravovye-osnovy-perevoda-okazaniya-gosudarstvennyh-uslug-v-elektronnyy-vid-na-primere-goroda-moskvy> (дата обращения: 28.05.2024).

12. Указ Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» от 07.05.2024 № 309 // Собрание законодательства РФ. – 2024. – №20.

13. Число пользователей «Госуслуг» составило 109 млн человек к концу 2023 года [Электронный ресурс] // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. – URL: <https://digital.gov.ru/ru/events/49226> (дата обращения: 25.02.2023).

В. Ф. Артюшкин,

кандидат политических наук, доцент,

Московский государственный институт международных отношений
(университет) Министерства иностранных дел Российской Федерации,

Е. А. Гусева,

преподаватель,

Московский государственный институт международных отношений
(университет) Министерства иностранных дел Российской Федерации,

Е. Ю. Ибрагимова,

преподаватель,

Московский государственный институт международных отношений
(университет) Министерства иностранных дел Российской Федерации

АНАЛИЗ СТАТИСТИКИ ПРЕСТУПНОСТИ ПО МЕТОДИКЕ ВИЗУАЛИЗАЦИИ МНОГОМЕРНЫХ СТРУКТУР

Аннотация. В статье предлагается к обычным методам анализа статистики преступности добавить методы многомерного корреляционного анализа и методики визуализации многомерных структур. Эти методы востребованы в задачах, в которых учитывается множество показателей независимо от их типа, величины и наличия перекрестных связей. Целью исследования является анализ преступности как системы и выявления особенностей в ее значимых изменениях. Исследования проводились по данным официальной статистики на основе 19 показателей во временном интервале с 1997 по 2022 г. В работе построены

плоские модели многомерных структур для нескольких наборов показателей: 7 качественных, 12 количественных, всех 19 и 6 альтернативных. Даны интерпретации результатов моделирования. Выявлены особенности в динамике состояний преступности, которые не проявлялись при использовании других методов.

Ключевые слова: системный анализ преступности, моделирование преступности, особенности динамики преступности

ANALYSIS OF CRIME STATISTICS ACCORDING TO THE METHOD OF VISUALIZATION OF MULTIDIMENSIONAL STRUCTURES

Abstract. The article proposes to add methods of multidimensional correlation analysis and methods of visualization of multidimensional structures to the usual methods of analyzing crime statistics. These methods are in demand in tasks that take into account a variety of indicators, regardless of their type, magnitude and the presence of cross-links. The purpose of the study is to analyze crime as a system and identify features in its significant changes. The research was conducted according to official statistics based on 19 indicators in the time interval from 1997 to 2022. In this paper, flat models of multidimensional structures for several sets of indicators are constructed: 7 qualitative, 12 quantitative, all 19 and 6 alternative. Interpretations of the simulation results are given. The features in the dynamics of crime conditions that did not manifest themselves when using other methods were revealed.

Keywords: systemic crime analysis, crime modeling, features of crime dynamics

Введение. Показатели преступности дают важную и разнообразную информацию о социально-политической ситуации в государстве. Группа показателей преступности, которая отслеживается статистикой, конечно, менялась со временем в соответствии с проблемами, возникающим в обществе, но она всегда наследовала достоинства и недостатки системного описания социального явления. В нее входят показатели не только неравнозначные по степени обобщения, но и разные по типу – количественные и качественные. Это позволяет проводить разнообразные исследования и ставить в них разные по сложности вопросы. Трудности начинаются тогда, когда поставленный вопрос требует анализа группы показателей.

Наиболее сложным является рассмотрение группы факторов как целого, как системы, в которой влияние каждого показателя учитывается на «равноправной» основе. К математическим методам, которые можно использовать для исследования таких системных задач, относятся методы многомерного шкалирования. Они являются научным аппаратом, позволяющим взглянуть на конфигурацию данных, неподвластную воображению человека. В моделях эти картины будут представлены искаженными, но даже в искаженных картинах обнаруживаются фрагменты, которые могут помочь нашему пониманию социального явления.

Основная часть. Чаще всего исследования статистики правонарушений связаны с анализом временных рядов статистики различных показателей преступности [4]. В работе мы покажем, какую дополнительную информацию можно получить, если стандартные подходы дополнить редко используемыми мето-

дами множественного корреляционного анализа и многомерного шкалирования [5].

После прекращения выпуска статистического сборника «Россия в цифрах» в 2021 г. сбор статистической информации для исследований усложнился. Теперь приходится обращаться к нескольким источникам. В основном, это по-прежнему сайт Федеральной службы государственной статистики¹³, а информация за последние годы (после 2018 г.) доступна на сайте Генеральной прокуратуры¹⁴.

Перечень отобранных для проведения исследований 12 количественных и 7 качественных показателей вместе с их условными обозначениями приведен в табл. П1, а сами значения в табл. П2 Приложения. Одним из критериев отбора показателей была непрерывность данных на всем выбранном временном интервале (1997–2022 гг.).

Обратимся к методике визуализации многомерных структур [1, 5, 6]¹⁵. Вначале дадим ее краткое пояснение.

Предельный случай множественности это два показателя, значит, простое графическое представление на плоскости, т. е. изображение, построенное на двух осях, каждая из которых привязана к одному из показателей, можно назвать двумерной структурой, или структурой в двумерном пространстве. Тогда, например, временной график – это временная структура показателя.

Визуально человек может хорошо анализировать графические представления и при трех показателях (трехмерное, объемное представление), ведь мы живем в трехмерном мире, но на этом его способности и заканчиваются. Вообразить картину с учетом четырех показателей мы уже не можем, хотя для описания состояния сложных социальных явлений нам часто требуется гораздо большее количество показателей. Одним из способов решения проблемы визуализации является создание плоской модели многомерной картины. Избежать больших ошибок при таком переходе нельзя, однако выявить основные «геометрические» свойства в многомерной картине можно. Еще одной сложностью является интерпретация плоского модельного изображения.

В настоящее время методы многомерного шкалирования реализованы как стандартные процедуры в нескольких статистических пакетах, благодаря чему стали частью научного инструментария.

¹³ URL: <https://rosstat.gov.ru/folder/210/document/13212> и URL: https://rosstat.gov.ru/storage/mediabank/Soc_pol_2023.htm (дата обращения 25.07.2024).

¹⁴ URL: <https://epp.genproc.gov.ru/web/gprf/activity/statistics> и http://crimestat.ru/offenses_map (дата обращения: 25.07.2024).

¹⁵ Методика визуализации многомерных структур (ВМС) относится к классу методов многомерного шкалирования (ММШ). ММШ – одно из направлений количественно-качественных исследований в социальных науках. ММШ используется в настоящей работе в варианте методики визуализации многомерных структур. Методика была разработана еще в 1990-е годы рядом российских специалистов и использовалась для решения задач в области политологии и международных отношений.

Основным критерием при построении плоских моделей является совокупный минимум расхождений в расстояниях между объектами в многомерном и двумерном пространствах.

Особенно ценна методика ВМС ее нацеленностью на использование в системных исследованиях, поскольку показатели могут быть не только независимыми, но и разнородными. Там, где необходим анализ структуры множества объектов на множестве показателей, оказываются востребованными методы многомерного шкалирования.

Для демонстрации «необычности» плоского аналога многомерного изображения покажем, как трансформируется в плоскость известный с детства куб (рис. 1).

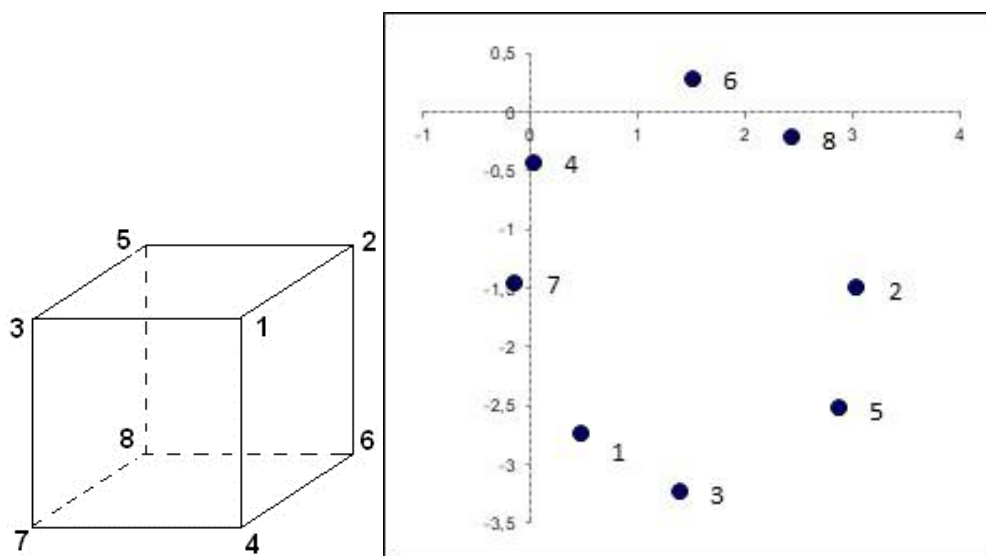


Рис. 1. Вершины трехмерного куба и модель их расположения на плоскости

Полезной является проверка работоспособности методики ВМС. Для этого выберем два показателя: «число мужчин из числа лиц, совершивших преступления» ($\{9\}$), и «число лиц, совершивших преступление возраста 18–24 гг.» ($\{13\}$). Коэффициент корреляции между ними равен 0,962.

В случае всего двух показателей вид структуры получаемой с помощью методики ВМС (рис. 2, справа)¹⁶ должен совпадать с графиком, который в популярной программе EXCEL называется «точечный», а в эконометрическом анализе «корреляционное поле» (рис. 2, слева). Идентичность рисунков подтверждает работоспособность методики ВМС.

¹⁶ Каждая точка левого графика на правом выглядит несколько иначе. Она принимает форму окружности, в которой соответствующий ее год отмечен только двумя последними цифрами, например, 2022 г. – как 22, а 1998 г. – как 98.

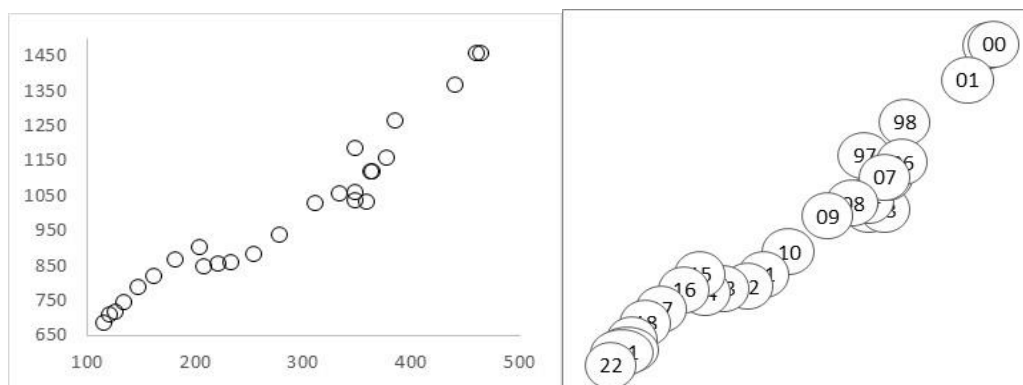


Рис. 2. Сравнение результатов использования метода ВМС для двухпараметрической модели и точечного графика

Точки на графике (рис. 2, слева) располагаются вдоль некоторой воображаемой прямой, что свидетельствует о сильной корреляционной (линейной) связи между показателями.

Модельное изображение структуры можно поворачивать и сдвигать относительно осей без ее изменения, поэтому на рис. 2 (справа) оно повернуто приблизительно на тот же угол наклона, что и у воображаемой прямой с левого графика. Перед процедурой оптимизации значения всех показателей нормируются в интервал (0; 1). Модельные оси являются всего лишь инструментальными. Они не связаны ни с одним показателем и служат только для демонстрации найденной оптимальной структуры. Инвариантность структуры относительно осей позволяет даже совсем отказаться от их показа.

Видимо уже понятно, что методологию ВМС мы предлагаем применить к состояниям преступности в разные моменты времени. Подход, при котором учитывается динамика структуры во времени уже апробирован. Например, в исследовании [6] образы страны на разных интервалах времени рассматривались как независимые объекты.

Задачи анализа временных рядов и построения структуры временных срезов, конечно, перекликаются, поскольку в обеих присутствует время, а следовательно, и динамика. Но в одной оно присутствует явным образом, поскольку исследуется временной ряд, в другой – косвенно, потому что анализируются временные срезы, и время присутствует как бы в контексте ситуаций. Однако картина временных срезов, конечно, не обязана давать простую графическую кривую, совпадающую с хронологией срезов.

Чтобы подчеркнуть особенности анализа структур, сравним уже полученную модель двух показателей {9} и {13} (рис. 3, слева) и модель, построенную для всех 12 количественных показателей – {8; 9; 10; 11; 12; 13; 14; 15; 16; 17; 18; 19} (рис. 3, справа). Для удобства сравнения они оба представлены на одном рис. 3.

Явно выраженные различия изображений являются результатом того, что каждый рассматриваемый показатель на «равноправных» основаниях определяет конфигурацию структуры. А сохранение некоторой направленности в расположении точек, говорит о том, что большинство показателей имеет линейную связь с обобщенным количественным показателем — «число выявленных лиц, совершивших преступления – всего».

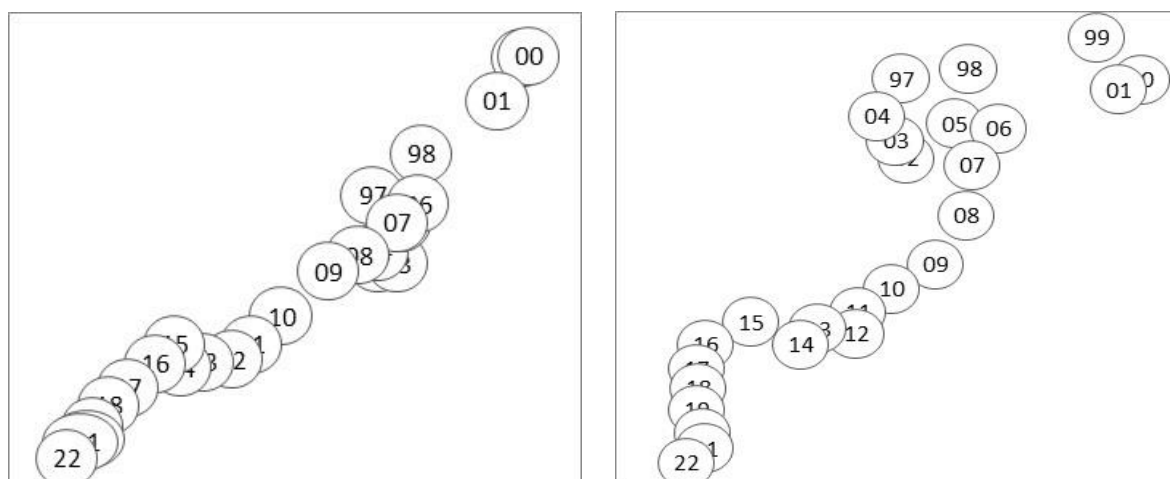


Рис. 3. Сравнение моделей с двумя и двенадцатью количественными показателями

С позиций эконометрики, наверно, можно сказать, что многомерная структура – это своего рода многомерное корреляционное поле с информацией о преобладающих зависимостях между показателями.

Теперь посмотрим, как выглядит структура с учетом всех 19 показателей (12 количественных показателей и 7 качественных). Для удобства восприятия здесь и далее все структуры повернуты так чтобы воображаемая линия, соединяющая первое состояние (условно обозначенное на рисунках как 97) и последнее (22) совпадала с направлением оси OX (рис. 4).

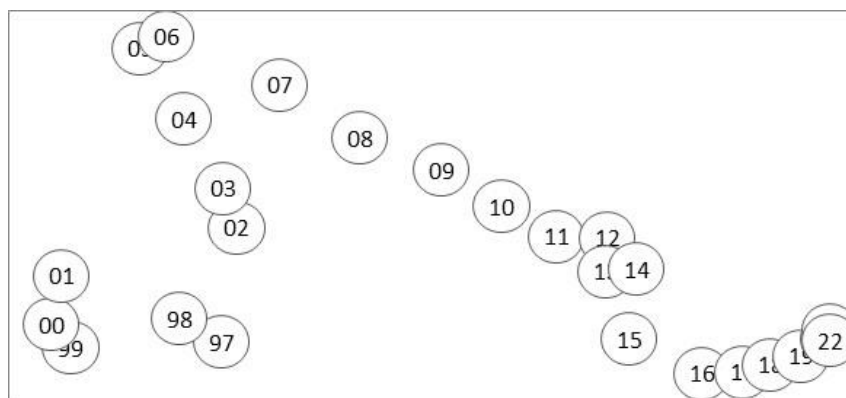


Рис. 4. Модель структуры для всех 19 показателей

Вариант интерпретации полученной структуры может быть следующим. При этом в качестве подтверждения своих выводов курсивом мы приводим значимые исторические события соответствующего времени [4, С. 130–131].

В начале отметим разнесение первых пяти лет наблюдения на два кластера. Причем кластер 1999–2001 гг. занимает одну из крайних позиций и таким образом указывает на некоторую уникальность состояния преступности в эти годы. *В 1999 г Б. Н. Ельцин покидает пост президента. В 2000 г президентом избран В. В. Путин. В 2000 г заканчивается Вторая чеченская война. С началом нового*

тысячелетия начинается постепенный рост мировых цен на энергоносители. Интересно отметить, что кластер 1997–1998 гг. находится гораздо ближе к 2002 г., значит в 2002 г. система резко поменяла не только свое состояние, но и направление изменений.

Следующее, что явно выделяется на рис. 4, – это последовательное хронологическое выстраивание временных срезов начиная с 2002 г. В 2002 г. в России вступают в силу новые Уголовно-процессуальный кодекс Российской Федерации, Трудовой кодекс Российской Федерации и Кодекс Российской Федерации об административных правонарушениях, а в 2003 г. и – Гражданский процессуальный кодекс. Таким образом, в 2003 г. была завершена реформа уголовного процессуального законодательства. Значит хронологическое выстраивание срезов отражает процесс «перезапуска» судебной системы на новых основаниях. Необходимо подчеркнуть, что столь явное указание на начало нового этапа в состоянии преступности в 2002–2003 гг. от их типа, величины и наличия перекрестных связей. На «донастройку» системы в практической работе ушло 3–4 года, и она была завершена к 2006 г.

После этого все элементы судебной системы начинают работать в хорошем согласовании друг с другом. Вначале ситуация изменяется быстро, но понемногу замедляется (траектория 06–11). В 2012–2014 гг. изменения приостанавливаются. В 2011–2013 гг. в Москве многократно проходят массовые политические выступления. В 2013–2015 гг. – пенсионная реформа. В 2015–16 гг. переход системы в новое стартовое состояние. В 2014–2016 гг. в России социально-экономический кризис на фоне падения мировых цен на энергоресурсы.

В 2016 г. стартует новый процесс изменений в состоянии преступности. Он длится до 2021 г. и проходит почти с одинаковым годовым темпом в согласованной работе элементов системы. В 2022 г. процесс изменений приостанавливается. В 2022 г. начинается СВО и происходит очень много значимых трансформаций в жизни страны.

Для полноты анализа и лучшего понимания произошедшего добавим еще несколько моделей. Во-первых, модель качественных (рис. 5) и модель количественных (рис. 6) показателей (для 12 количественных показателей модель уже показана, мы просто представим ее в оговоренной ориентации).

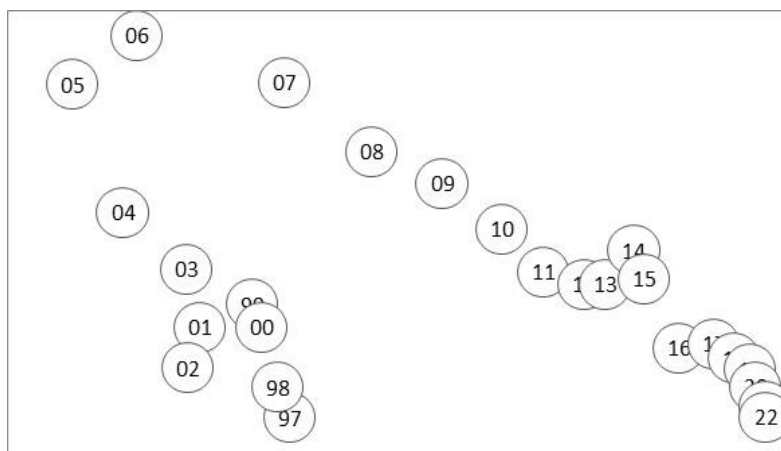


Рис. 5. Модель структуры для 7 качественных показателей

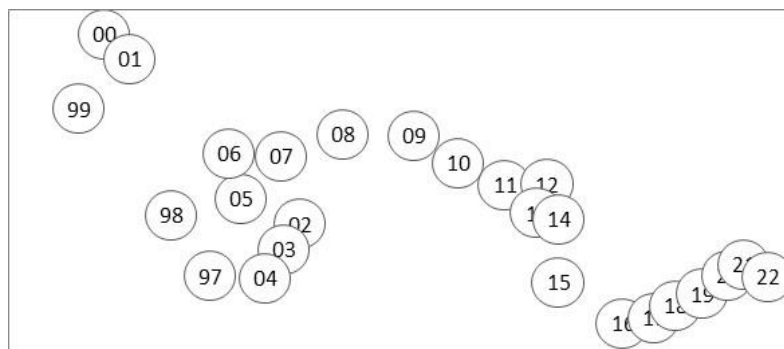


Рис. 6. Модель структуры для 12 количественных показателей

Из этих моделей выделим только элементы, существенно отличающие их от модели с полным составом показателей.

В модели качественных показателей переход системы на новые принципы существования происходит не в 2002 г., а в 2003 г. Процесс приостановки изменений в 2012–2014 гг. продлевается и на 2015 г. Новый процесс изменений 2016–2021 гг. проходит почти по той же траектории, что и в 2007–2011 гг. Остается получить обоснование этим особенностям в статистике качественных показателей.

В модели количественных переменных есть большой кластер, в котором и кластер начала наблюдений 1999–1998 гг. и расширенный период становления правовой системы 2002–2007 гг., т. е. с точки зрения количественных показателей состояния системы в эти годы структурно однотипны. А процесс изменений начинается не с 2006 г., а с 2008 г. И здесь есть место дополнительному анализу статистики количественных показателей.

Еще одной интересной задачей, которая логически возникает после моделирования с разными наборами показателей, является задача сокращения их количества и тем самым сокращения размерности пространства.

При какой наименьшей группе показателей получается структура, близкая к структуре полного набора показателей? Для поиска такого набора необходимо определить критерий близости, но четкого формального критерия здесь нет, поэтому предлагаемый нами вариант не является однозначно лучшим. Хорошее приближение достигается группой из 6 показателей следующего состава: [4, 10, 11, 12, 13, 14]. Все эти показатели оказались показателями количественного типа. Их модельная структура показана на рис. 7, по ней можно убедиться в близости структур.

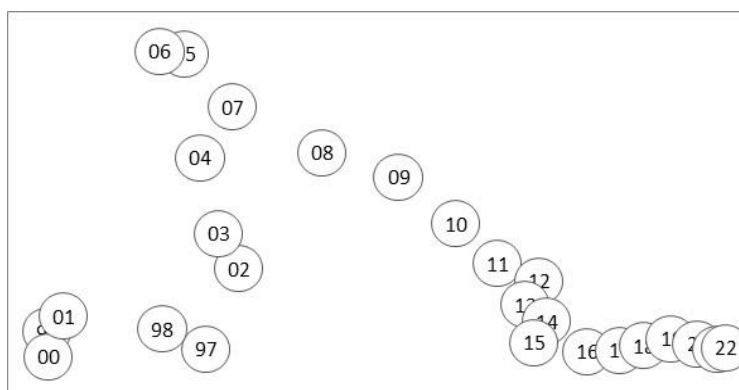


Рис. 7. Модель структуры для минимальной группы из 6 показателей

Этот результат является неожиданным. Ведь модель 7 качественных показателей более похожа на модель с полным набором, чем модель с 12 количественными показателями, однако минимальная группа оказалась только с качественными показателями.

Сокращение размерности, которое возможно провести, опираясь на полученный результат, конечно, не решает проблемы визуализации. Но она может быть полезна при решении трудностей в сборе статистики для проведения исследований.

Для глубокого и разностороннего понимания преступности и слежения за процессами ее изменений статистика накапливает данные по множеству показателей. Стандартный комплекс задач анализа обычно решается стандартным набором математических методов. Однако расширение математического инструментария позволяет не только открывать новую информацию, но и ставить новые задачи исследований. Это, прежде всего, относится к методам, не предполагающим получение уравнений связи между показателями и факторами.

Главным посылом работы является призыв к использованию в анализе преступности методики визуализации многомерных структур. Визуализация в виде плоской модели той структуры, которая выстраивается в многомерном пространстве показателей, позволяет лучше понять системность объекта исследований. Объектами анализа выступали значения показателей преступности в разные годы, т. е. временные срезы состояния преступности.

Применение методологии ВМС позволило выявить интересные особенности изменений в состояниях преступности во времени, причем с учетом влияния всех показателей независимо от их типа, величины и наличия перекрестных связей.

Приложение
Таблица П1

Показатели преступности

Обозначение показателя	Показатель
<i>Число зарегистрированных преступлений:</i>	
{1}	Убийство и покушение на убийство
{2}	Умышленное причинение тяжкого вреда здоровью
{3}	Изнасилование и покушение на изнасилование
{4}	Грабеж
{5}	Разбой
{6}	Кража
{7}	Преступления, связанные с незаконным оборотом наркотиков
{8}	Число лиц, содержащихся в местах лишения свободы, тыс. человек
<i>Выявлено лиц, совершивших преступления, по полу:</i>	
{9}	Мужчины
{10}	Женщины

Обозначение показателя	Показатель
<i>Выявлено лиц, совершивших преступления, по возрасту:</i>	
{11}	14–15
{12}	16–17
{13}	18–24
{14}	25–29
{15}	30–49
{16}	50 и более
<i>Выявлено лиц, совершивших преступления, по занятию:</i>	
{17}	Учащиеся и студенты
{18}	Лица без постоянного источника дохода
{19}	Безработные

Таблица П2

Статистические ряды показателей преступности (в тысячах)

	{1}	{2}	{3}	{4}	{5}	{6}	{7}	{8}	{9}	{10}	{11}	{12}	{13}	{14}	{15}	{16}	{17}	{18}	{19}
1997	29,3	46,1	9,3	112,1	34,3	1054	184,8	1018	1186	186	45,9	116	349	215	567	78,4	81,8	719	73,2
1998	29,6	45,2	9,0	122,4	38,5	1143	190,1	1015	1264	218	46,8	118	385	238	607	86,4	88,3	798	78
1999	31,1	47,7	8,3	139,0	41,1	1414	216,4	1060	1456	261	51,2	132	461	282	683	108	105	954	81,4
2000	31,8	49,8	7,9	132,4	39,4	1310	243,6	925	1457	284	49,3	129	465	289	676	133	101	954	91,4
2001	33,6	55,7	8,2	148,8	44,8	1273	241,6	980	1365	279	51,9	121	441	273	625	132	94,3	906	85,8
2002	32,3	58,5	8,1	167,3	47,1	927	189,6	877	1035	223	40,1	100	348	199	463	108	77,7	658	63,3
2003	31,6	57,1	8,1	198,0	48,7	1151	181,7	847	1031	206	43,2	102	359	200	436	96,1	82	664	65,9
2004	31,6	57,4	8,8	251,4	55,4	1277	150,1	763	1059	163	46	106	348	202	425	96,3	85,8	719	73,1
2005	30,8	57,9	9,2	344,4	63,7	1573	175,2	823	1119	178	44,6	105	365	224	454	106	87,1	782	82
2006	27,5	51,4	8,9	357,3	59,8	1677	212,0	872	1156	205	44,1	104	378	242	478	114	90,1	811	84,1
2007	22,2	47,3	7,0	295,1	45,3	1567	231,2	883	1117	201	38,1	93,9	363	238	470	115	83,8	785	74,5
2008	20,1	45,4	6,2	244,0	35,4	1326	232,6	888	1055	201	29,6	78,3	334	230	470	114	91	764	67,3
2009	17,7	43,1	5,4	205,4	30,1	1189	238,5	864	1026	194	23,7	61,8	312	228	479	115	77,7	786	55,1
2010	15,6	39,7	4,9	164,5	24,5	1108	222,6	819	939	172	21,5	51,2	278	209	448	103	72	730	54,3
2011	14,3	38,5	4,8	127,8	20,1	1039	215,2	756	882	159	20,5	45,5	254	194	433	94,6	64,7	691	47,2
2012	13,3	37,1	4,5	110,1	18,6	992	219,0	702	857	154	18,5	41	234	192	432	93,9	59,2	675	45,4
2013	12,4	34,8	4,2	92,1	16,4	923	231,5	677	856	156	19,7	41	222	192	441	97,3	60,9	665	38,1
2014	11,9	32,9	4,2	77,7	14,3	909	254,7	666	848	158	17,1	37,3	208	190	455	99,2	54,9	663	35
2015	11,5	30,2	3,9	72,7	13,6	1019	236,9	640	903	172	17,2	38,8	204	202	504	110	56	717	22
2016	10,4	27,4	3,9	61,5	11,4	871	201,2	630	868	148	15,6	33	182	193	483	109	50	665	6,1
2017	9,7	24,6	3,5	56,9	9,1	789	208,7	602	820	147	14,9	27,6	162	172	484	107	45,5	636	4,4
2018	8,6	23,2	3,4	50,1	7,5	756	200,3	563	786	145	14,8	26	148	153	482	108	44,4	601	4,8
2019	7,9	21,5	3,2	45,8	6,7	774	190,2	524	742	143	13,8	24,2	135	135	472	105,1	40,9	564	4,9
2020	7,6	20,0	3,5	38,4	5,3	751	189,9	482	716	136	11,4	22,2	126	123	466	103,8	34,8	545	7,6
2021	7,3	17,9	3,5	31,5	4,4	733	179,7	466	711	138	9,5	19,6	122	113	479	105,9	31,2	544	8,6
2022	7,6	17,4	3,3	29,2	4,0	698	177,7	418	686	134	8,7	17,7	116	102	470	105	28,1	531	4,1

Список литературы

1. Артюшкин, В. Ф. Соотношение сил между великими державами в «Группе 20»: анализ при помощи метода многомерного шкалирования / В. Ф. Артюшкин, А. А. Казанцев, В. М. Сергеев // Полис. Политические исследования. – 2021. – № 2. – С. 125–138. – DOI 10.17976/jpps/2021.02.09. – EDN JMFZKC.
2. Артюшкин В. Ф., Токарева В. И. К вопросу о моделировании динамики преступности в России // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции В 6 т., Казань, 22 сентября 2023 года. – Казань: Познание, 2023. – С. 126–136.
3. Артюшкин В. Ф., Токарева В. И., Звягинцев М. М. Динамика преступности в России – модельный анализ // Право и управление. XXI век. – 2024. – Т. 20, № 1(70). – С. 188–198. – DOI 10.24833/2073-8420-2024-1-70-188-198. – EDN CBLGCZ.
4. Богданова М. В., Паршинцева Л. С., Квачко И. Ю. Методика моделирования и прогнозирования преступности в Российской Федерации // Правовая информатика. – 2019. – № 4. – С. 50–62.
5. Дэйвисон М. Многомерное шкалирование. Методы наглядного представления данных. М.: Финансы и статистика, 1982.
6. Sanidas E. Evidence of the Strong Nexus between Economic, Social, Business, and Political Indicators across the World // International Journal of Economics & Management Sciences. 2017. Vol. 6, № 6. <https://doi.org/10.4172/2162-6359.1000481> (дата обращения: 30.07.2024).

А. А. Беляева,

магистрант,

Московский государственный университет
имени М. В. Ломоносова (филиал в г. Сарове)

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ДЛЯ ПОСТРОЕНИЯ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ДИНАМИКИ ЭЛЕКТРОНОВ В СИНХРОТРОНЕ

Аннотация. Целью данной работы является анализ программных средств, предназначенных для моделирования динамики пучков электронов в накопительном кольце синхротронной установки, в частности программы MAD-X. В работе рассматриваются история создания ускорительных установок, принципы математического моделирования периода накопительного кольца синхротрона на основе линейной модели (уравнения Хилла, теорема Флоке, матричный формализм), а также возможности моделирования, предоставляемые комплексом программ MAD-X. Учитывая сложность разработки оборудования, необходимого для создания синхротронного излучения, важную роль приобретают математические расчеты, обеспечивающие тонкую настройку синхротронной установки.

Ключевые слова: динамика пучка, синхротронное излучение, ускорительно-накопительный комплекс, моделирование ускорителя, комплекс программ, линейная модель, матричный формализм

THE USE OF DIGITAL TECHNOLOGIES TO BUILD A MATHEMATICAL MODEL OF THE DYNAMICS OF ELECTRONS IN A SYNCHROTRON

Abstract. The work objective is to analyze software for modeling dynamics of electron beams in a synchrotron accumulator ring, in particular MAD-X software. The work considers the history of accelerators, the principles of mathematical modeling of the synchrotron accumulation ring period based on linear model (Hill's equation, Floquet's theorem, matrix formalism), as well as the possibilities of modeling provided by MAD-X software. Given the complexity of developing the equipment for synchrotron radiation, of particular importance are the mathematical calculations, which ensure a fine adjustment of the synchrotron complex.

Keywords: beam dynamics, synchrotron radiation, fast-track accumulation complex, accelerator modelling, software package, linear model, matrix formalism

Введение. Ускорители заряженных частиц – это устройства для получения заряженных частиц высоких энергий. Крупные ускорители являются дорогостоящими комплексами, их создание и эксплуатация требуют международного сотрудничества. Результаты исследований, которые становятся возможными при использовании подобного оборудования, вносят неоценимый вклад в науку.

К примеру, Большой адронный коллайдер (БАК), расположенный в Европейском Центре ядерных исследований (ЦЕРН), представляет собой кольцо длиной почти в 27 километров и является результатом работы десятков тысяч ученых из более чем ста стран. В ходе экспериментов, проведенных на этом ускорителе, была открыта частица – бозон Хиггса, обнаружено несколько новых видов кварков и других частиц, получены ранее неизвестные данные, характеризующие взаимодействия протонов между собой и с другими частицами, и многое другое.

Расчетам движения заряженных частиц в ускорительных установках посвящено множество статей известных зарубежных и отечественных авторов. В данной работе исследуется динамика движения пучка электронов на основе коррекции коэффициентов матриц перехода уравнения Хилла с учетом специфики синхротронной ускорительной установки. Актуальность этого направления связана с возможностью применения данного метода для дальнейшего анализа динамики пучков заряженных частиц в различных ускорительных установках и решения множества прикладных задач, связанных с транспортировкой пучков заряженных частиц.

В данной работе рассматривается движение пучка электронов в синхротроне. Динамика частиц рассматривается на основе линейной модели. Все магнитные элементы описываются как приближенные к идеальным, с постоянными полями без учета краевых эффектов.

Основная часть. Существуют различные виды ускорительных установок [7]. Многие из них активно эксплуатируются и в настоящее время, поскольку от конструкции установки в немалой степени зависят параметры результата ра-

боты прибора: пучка, излучения, состояния частиц. Рассмотрим подробнее историю [3] создания и развития ускорительных установок.

В настоящий момент конструкция существующих ускорителей непрерывно совершенствуется, разрабатываются и внедряются новые инженерные решения, направленные на улучшение фокусировки пучка заряженных частиц в накопительном кольце, повышение стабильности его траектории, а также другие задачи, возникающие в процессе моделирования транспортировки пучков заряженных частиц в ускорительных установках [6]. Таким образом, увеличивается коэффициент полезного действия всей установки, а также появляются возможности для проведения новых, более точных экспериментов с использованием таких продуктов работы ускорительных установок, как, например, синхротронное и бетатронное излучения.

По назначению ускорители заряженных частиц делятся на промышленные, медицинские, ускорительные масс-спектрометры, источники синхротронного излучения, коллайдеры и лазеры на свободных электронах [13]. Они находят применение в промышленной и медицинской сферах, масс-спектрометрия используется для определения химического, изотопного и элементного состава вещества. Синхротронное излучение применяется в самых разных областях науки. Коллайдеры в основном используются с целью изучения процессов столкновения частиц высоких энергий, лазеры на свободных электронах – как специализированный источник когерентного рентгеновского излучения.

По конструкции ускорители делятся на линейные и циклические. К линейным относятся: высоковольтный, линейный резонансный и линейный индукционный ускорители. Среди богатого разнообразия циклических ускорителей выделяют бетатрон, циклотрон, микротрон, фазотрон (также известный как синхроциклотрон), синхрофазотрон, ускоритель-рекуператор и синхротрон.

В этой работе рассматривается синхротрон. Эта установка представляет собой резонансный циклический ускоритель, источник синхротронного излучения.

С развитием науки и технологий синхротронное излучение стало активно использоваться в различных областях. К примеру [18], в 2020-м году при помощи синхротронного излучения были просканированы с впечатляющей детализацией эмбрионы динозавров, находящиеся в яйцах. Было чрезвычайно важно использовать не разрушающий метод сканирования, другие виды сканирования не подходили под требования. По результатам этого исследования была восстановлена схема эмбрионального развития динозавров. Также [22] при помощи синхротронного излучения и метода рентгеновской кристаллографии ученые могут узнать пространственное строение белка. Это помогает создавать соединения, регулирующие функции белков, то есть создавать фармацевтические препараты с новыми или усиленными свойствами.

Важным элементом синхротронного ускорителя является накопительное кольцо, которое содержит магнитные элементы, непосредственно влияющие на характеристики пучка заряженных частиц: его траекторию, дисперсию и проч. Рассмотрим подробнее эволюционный путь квадрупольных магнитов.

Изобретение квадрупольной линзы позволило науке значительно продвинуться в методах транспортировки пучков заряженных частиц. Благодаря им стала возможной реализация принципа жесткой фокусировки. В дальнейшем со-

здание квадрупольных масс-анализаторов дало толчок масс-спектрометрии. В 1953 году немецким ученым Вольфгангом Паулем был описан первый прибор с высокочастотным квадрупольным анализатором. С развитием техники масс-спектрометры уменьшились в размерах, стали проще в эксплуатации и доступнее для широкого круга пользователей. В конце 1960-х годов советские физики И. М. Капчинский и В. А. Тепляков [21] изобрели ускоритель ионов на основе высокочастотного квадруполя. В настоящее время ускорители с высокочастотной квадрупольной фокусировкой широко используются в ускорительных лабораториях [4], ведутся разработки более совершенных моделей магнитов [8].

Для расчетов устройств электронной оптики и каналов транспортировки пучков заряженных частиц разработаны и активно используются многочисленные компьютерные программы. Зачастую они основаны или на применении матричного метода расчета каналов транспортировки пучков (программа TRANSPORT и ее потомки, например, MAD), или на решении уравнения движения частиц в параксиальном приближении (PARMELA, ASTRA и т. п.). Самостоятельное освоение таких программ и правильная интерпретация полученных результатов требуют серьезной предварительной подготовки: знания многих разделов теоретической физики и высшей математики. Также необходимо отчетливое представление о физических процессах, протекающих в устройствах транспортировки пучков.

В данной статье рассматривается синхротронный ускоритель частиц, который представляет собой источник синхротронного излучения 4-го поколения [1, 9, 15–17, 20]. Подобный прибор, Европейский источник синхротронного излучения (ESRF) [19, 23], уже был построен и успешно запущен в 2020 году в Гренобле (Франция). ESRF – самый высокоэнергетичный синхротрон среди европейских источников синхротронного излучения. В этом ускорителе используются высококоэрцитивные постоянные магниты, что обеспечивает стабильную работу установки, поскольку такие магниты отличаются стабильностью своих свойств: создают магнитное поле с постоянным напряжением и тяжело размагничиваются.

Синхротрон – это кольцевой циклический ускоритель заряженных частиц, то есть электровакуумная установка с приблизительно кольцевой вакуумной камерой, в которой поток частиц, в данном случае электронов, минимально теряя энергию, удерживается на фиксированной орбите с помощью поля мощных отклоняющих и фокусирующих его кольцевых магнитов. Синхротрон состоит из инжектора, линейного ускорителя и накопительного кольца. Накопительное кольцо состоит из повторяющихся участков, суперпериодов, включающих в себя как магнитные (диполи, квадруполи, секступоли и т. д.), так и другие (промежутки, мониторы, корректоры, ВЧ-резонаторы) элементы. Рассматриваемая установка содержит n суперпериодов, на каждом из которых пучок совершает поворот на $\frac{360}{n}$ градусов. Синхротронное излучение выводится с каждого такого элемента накопительного кольца в виде сфокусированного луча.

Разберем подробнее принцип действия синхротронной установки. Пучок электронов выбрасывается из ускорительной установки в накопительное кольцо, и порождаемое им синхротронное излучение, которое излучается частицами

в направлении по касательной к окружности накопительного кольца, перенаправляется на научно-исследовательские станции, расположенные вокруг установки, для дальнейшего использования.

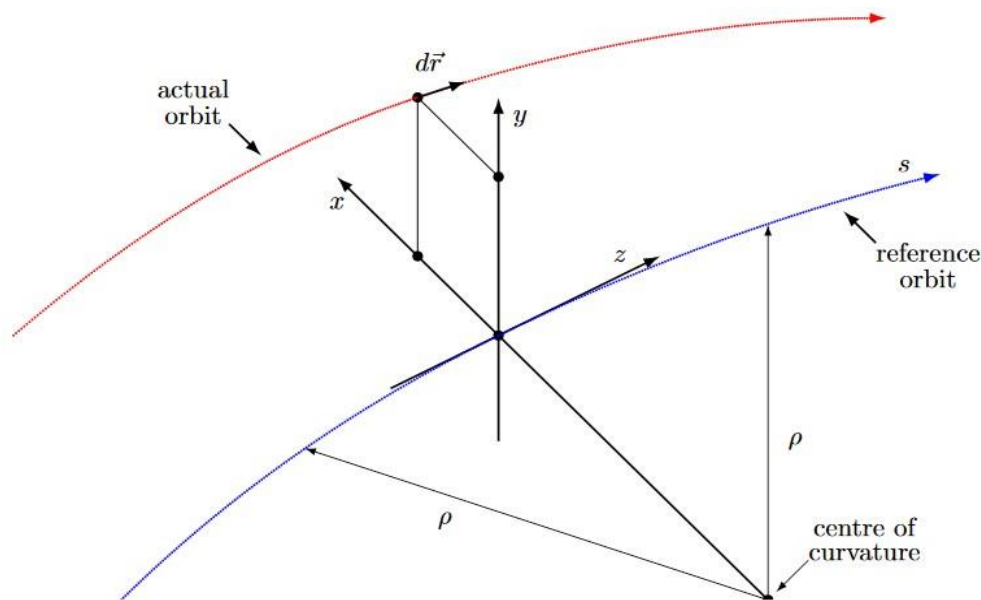


Рис. 1. Равновесная орбита в принятой системе координат

Источник: [24].

Движение заряженной частицы описывается уравнением Ньютона-Лоренца, общим уравнением движения заряженной частицы в магнитном поле, представленным ниже:

$$\frac{d\vec{p}}{dt} = e\vec{E} + \frac{e}{c}[\vec{v}, \vec{B}], \quad (1)$$

где p – импульс частицы, E и B – вектора напряженности электрического и магнитного полей соответственно, e – величина электрического заряда частицы, c – скорость света в вакууме.

Для моделирования динамики пучка заряженных частиц в ускорительной установке может использоваться комплекс программ MAD-X [24].

MAD-X – это комплекс программ, предназначенный для проектирования оптики заряженных частиц и проведения исследований при помощи моделирования ускорителей и пучков заряженных частиц.

MAD-X основан на языке C++, это обеспечивает высокую скорость его работы, что является очень важной характеристикой для подобной программы, поскольку моделирование пучка частиц требует обработки большого массива данных.

Существуют библиотеки, которые позволяют интегрировать пакет MAD-X в различные языки программирования. В частности, для Python такая библиотека называется *срумад* (1.9.3) [10]. *Срумад* позволяет передавать данные между MAD-X и вспомогательными модулями, к примеру, подпрограммой генерации графиков параметров функции Твисса, напрямую, без промежуточного хранения файлов.

Все магнитные элементы (диполи, квадруполи и т. д.) описываются при помощи встроенных функций и команд. В качестве исходных данных функции Твисса используются: начальные значения бета-функций (по осям x и y), начальное значение дисперсии (по одной из осей), значения энергии и соответствующей жесткости поля, оптическая схема регулярного периода накопительного кольца ускорительной установки. MAD-X может учитывать как тип ускорительной установки, так и тип ускоряемых частиц. К примеру, при рассмотрении синхротронной установки энергия и жесткость поля остаются неизменными для каждой точки возможной траектории частиц. Команда «`BEAM, PARTICLE = »` («ПУЧОК, ЧАСТИЦА = ») принимает в качестве входных данных как встроенные типы частиц, то есть, по умолчанию, позитрон, а также протон, электрон, антипротон и др., так и ионы, массу и заряд которых пользователь может ввести самостоятельно. Оптическая схема должна содержать характеристики и расположение магнитов на протяжении всего периода. Период накопительного кольца представляет из себя часть окружности накопительного кольца и может содержать пролетные промежутки и различные виды магнитов: диполи, квадруполи, секступоли, октуполи и др. Длина каждого элемента, а также напряжения полей магнитов известны.

Моделирование магнитных элементов происходит с использованием обобщенных уравнений матриц. Графики параметров функции Твисса могут быть построены с применением программы на языке Python, в таком случае в качестве данных для построения функции используется массив, сформированный в MAD-X при помощи команды «`select, flag=twiss, column=name, s, betx, alfx, bety, alfy;`». Массив будет содержать названия и длину элементов суперпериода (пролетных промежутков, магнитов и проч.), а также значения альфа- и бета-функций в точках изменения типа элемента модели. Бета-функции строятся с учетом линейности модели каждого элемента системы.

Построенные таким образом графики бета-функций отражают оптические характеристики канала накопительного кольца. По теореме Флоке, в области устойчивости существует функция с периодическим модулем, который полностью описывает пропускную способность канала. Для описания положения частиц в поперечной плоскости канала используются обе бета-функции, соответствующие горизонтальным (по оси x) и вертикальным (по оси y) колебаниям пучка, поскольку эта пара функций характеризует оптический канал.

Линейность движения частиц в каждой из областей действия магнитных элементов порождает следующие свойства этого движения:

1. Частота колебаний частицы одинакова для всех частиц пучка и не зависит от амплитуды колебаний.
2. Фазовые траектории частицы – эллипсы или, при соответствующем выборе фазовых переменных, окружности.
3. Если движение частицы удовлетворяет условиям устойчивости, то оно будет устойчиво при любой амплитуде колебаний частицы. Область финитного движения задают механические ограничения (элементы вакуумной камеры).

Смоделированные бета-функции будут отражать амплитуду бетатронных колебаний пучка заряженных частиц. При помощи функций некоторых библиотек (в Python для линейной модели «`np.trapz()`») можно также рассчитать пло-

щадь под графиками полученных бета-функций, а следовательно, и эмиттанс пучка. Последняя характеристика описывает сфокусированность пучка, то есть является критерием или одним из критериев качества модели для множества задач в области моделирования ускорителей [12].

Однако ничто из обозначенного выше не гарантирует, что полученные функции параметров функции Твисса будут симметричными [5]. Если бета-функции не будут симметричными, это означает, что оптическая модель ускорителя с данными характеристиками магнитов не обеспечивает фокусировку пучка и происходит его рассеивание. Чтобы предотвратить это, необходимо провести оптимизацию модели [2] при помощи математических методов и провести повторное моделирование в программе MAD-X, чтобы проверить сделанное предположение. Поскольку моделируется лишь период ускорительной установки, который далее повторяется n раз, образуя замкнутую структуру ускорителя, симметричность бета-функций необходима для устойчивой фокусировки пучка частиц.

Заключение. Исходя из изложенного выше, можно сделать следующие выводы:

1. При помощи дополнительной программы, написанной на языке Python или другом языке программирования, можно построить графики полученных параметров функции Твисса, а также рассчитать интеграл полученной функции и, следовательно, эмиттанс пучка.

2. Характеристики модели ускорительной установки могут быть улучшены посредством оптимизации параметров составляющих ее элементов, в частности магнитов. Данные исследования могут быть использованы для дальнейшего анализа динамики пучков частиц в ускорительных установках и решения связанных с этим прикладных задач.

Список литературы

1. Ашанин И. А., Ключевская Ю. Д., Махоро А. А. и др. Динамика пучка в линейном ускорителе-инжекторе специализированного источника синхротронного излучения 4-го поколения ИССИ-4 // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. – 2019. – Т. 15. – С. 126–139.

2. Баранов Г. Н., Богомягков А. В., Левичев Е. Б., Синяткин С. В. Оптимизация магнитной структуры источника синхротронного излучения четвертого поколения СКИФ в Новосибирске. // Сибирский физический журнал. – 2020. – Т. 15, № 1. – С. 5–23.

3. Баранов М. И. Антология выдающихся достижений в науке и технике. Часть 8: Создание ускорителей заряженных частиц // Электротехника и электромеханика. – 2012. – № 3. – С. 3–9.

4. Беляев О. К., Буданов Ю. А., Звонарев И. А. Линейный ускоритель тяжелых ионов с высокочастотной фокусировкой [Электронный ресурс] // Физика и техника ускорителей. Письма в ЭЧАЯ: [сайт]. – URL: http://www1.jinr.ru/Pepan_letters/panl_2013_7/29_bel.pdf (дата обращения: 25.08.2024).

5. Беляева А. А., Князев Н. А. Влияние модификаций вычислительных моделей постоянных дипольных магнитов источника синхротронного излучения на оптические характеристики пучка заряженных частиц // Процессы управления и устойчивость. – 2024. – Т. 11, № 1. – С. 71–80.
6. Бенфорд А. Транспортировка пучков заряженных частиц: пер. с англ. – М.: Атомиздат, 1969. – 240 с.
7. Брук Г. Циклические ускорители заряженных частиц: пер. с франц. – М.: Атомиздат, 1970. – 313 с.
8. Быков С. А., Востриков В. А., Жилиев К. В., Морозов И. И., Окунев И. Н., Пахомов А. Ю. Исследование квадрупольных линз для канала транспортировки ионов // Сибирский физический журнал. – 2023. – Т. 18, № 4. – С. 5–19. – DOI: <https://doi.org/10.25205/2541-9447-2023-18-4-5-19>
9. Воробьев Д. С., Куксанов Н. К., Домаров Е. В., Голубенко Ю. И., Корчагин А. И., Салимов Р. А., Фадеев С. Н., Чакин И. К., Семенов А. В., Лаврухин А. В., Потапова Ю. Э. Новейшие модели ускорителей ЭЛВ с энергией до 4 МэВ. // Сибирский физический журнал. – 2024. – Т. 19, № 2. – С. 80–87. – DOI: <https://doi.org/10.25205/2541-9447-2024-19-2-80-87>
10. Документация библиотеки cpyrpad [Электронный ресурс]. – URL: <http://hibtc.github.io/cpyrpad> (дата обращения: 25.08.2024).
11. Левичев Е. Б. Лекции по нелинейной динамике частиц в циклическом ускорителе: учеб. пособие. – Новосибирск: Изд-во НГТУ, 2009. – 224 с.
12. Максимов А. В., Новоскольцев Ф. Н., Синюков Р. Ю., Янович А. А. Моделирование и измерение эмиттанса пучков ионов углерода в канале радиобиологических исследований на ускорительном комплексе У-70. // Сибирский физический журнал. – 2024. – Т. 19, № 2. – С. 63–70. – DOI: <https://doi.org/10.25205/2541-9447-2024-19-2-63-70>
13. Пенюонжкевич Ю. Э. Современные ускорители заряженных частиц и их приложение // Вестник МАН РС. – 2021. – №1. – URL: <https://cyberleninka.ru/article/n/sovremennye-uskoriteli-zaryazhennyh-chastits-i-ih-prilozhenie> (дата обращения: 25.08.2024).
14. Сидорин А. О., Мешков И. Н. Транспортировка пучков заряженных частиц: учеб.-методич. пособие. – Дубна, 2013. – 192 с.
15. Юров Д. С., Шведун В. И., Алимов А. С. Линейные ускорители электронов непрерывного действия для научных и прикладных целей // Вестник Московского университета. Серия 3. Физика. Астрономия. – 2023. – №1. – URL: <https://cyberleninka.ru/article/n/lineynye-uskoriteli-elektronov-nepreryvnogo-deystviya-dlya-nauchnyh-i-prikladnyh-tseley> (дата обращения: 25.08.2024).
16. Arslanova D., Gavrish Y., Gaponok E., Grosheva A., Knyazev N., Kukhtin V., Lamzin E., Nezhentzev A., Ovsyannikov A., Ovsyannikov D., Sytchevsky S., Znamenshchikova N. Feasibility study of permanent magnet dipoles for SILA facility // Cybernetics and physics. – 2023. – № 12. – P. 252–256. – DOI: <https://doi.org/10.35470/2226-4116-2023-12-4-252-256>
17. Ashanin I. A., Polozov S. M., Pronikov A. I., Kliuchevskaia Yu. D. Beam dynamics simulation in a linear electron accelerator – injector for the 4th generation specialized synchrotron radiation source USSR // 27th Russian Particle Accelerator Conference. – 2021. – P. 149–152.

18. Chapelle K. E. J., Fernandez V. and Choiniere J. N. Conserved in-ovo cranial ossification sequences of extant saurians allow estimation of embryonic dinosaur developmental stages // Scientific Reports. – 2020. – Vol. 10. – DOI: <https://doi.org/10.1038/s41598-020-60292-z>
19. ESRF Upgrade Program Phase II [Электронный ресурс]. – URL: https://www.esrf.fr/Apache_files/Upgrade/ESRF-orange-book.pdf (дата обращения: 25.08.2024).
20. Fomin Ye., Korchuganov V. Kurchatov synchrotron radiation source – from the 2nd to the 4th generation // Russian Particle Accelerator Conference. – 2021. – P. 84–87.
21. Kapchinskiy I. M., Teplyakov V. A. The linear accelerator with spatially uniform strong focusing [Электронный ресурс] // Preprint ITP 673: [сайт]. – URL: <https://www.slac.stanford.edu/pubs/slactrans/trans01/slac-trans-0099.pdf> (дата обращения: 25.08.2024).
22. Polina V. Zhdanova, Alexander A. Ishchenko, Alexander A. Chernonosov, Dmitry O. Zharkov, Vladimir V. Koval. Dynamics and Conformational Changes in Human NEIL2 DNA Glycosylase Analyzed by Hydrogen/Deuterium Exchange Mass Spectrometry. // Journal of Molecular Biology. – 2022. – Vol. 434, Iss. 2. – DOI: <https://doi.org/10.1016/j.jmb.2021.167334>
23. Raimondi P. Hybrid multiband achromat: From Super B to EBS // In Proc. IPAC'17. – Copenhagen: Denmark. – 2017. – Pp. 3670–3675.
24. The MAD-X Program (user's guide) [Электронный ресурс]. – URL: <https://mad.web.cern.ch/mad> (дата обращения: 25.08.2024).

О. В. Богданова,
преподаватель,

Российский государственный социальный университет

СЕЛЕКЦИЯ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. Статья посвящена цифровизации семеноводства в условиях цифровых технологий и инноваций. Критически анализируются законодательство в сфере семеноводства и патентования и судебная практика по спорам, связанным с патентованием новых сортов растений. Обозначены положительные стороны этого прогресса.

Ключевые слова: агропромышленная политика, инновация, семена, реестр, производство, воспроизводство

BREEDING IN THE DIGITAL AGE

Abstract: This article is devoted to the digitalization of seed production in the context of digital technologies and innovations. The legislation in the field of seed production and patenting and judicial practice in disputes related to the patenting of new plant varieties are critically analyzed. The positive sides of this progress are indicated.

Keywords: agro-industrial policy, innovation, seeds, registry, production, reproduction.

Введение. Научно-техническая революция привела к прогрессу в технических и естественных областях знаний. Она сопряжена с созданием цифровых технологий и инноваций. Цифровые технологии легли в основу общественных технических процессов, которые протекают в наши дни в обществе. XXI век немыслим без технологического прогресса и инноваций. Они направлены на прогресс и оперативное разрешение поставленных задач в соответствующей сфере и в разрешении конкуренции.

Цифровые технологии задействованы на всех этапах производств и во всех сферах жизни человека: здравоохранение, образование, промышленность и производство. Цифровые технологии и цифровизация напрямую связаны с научно-биологическим развитием, который имеет свое поступательное движение. Цифровизация не обошла стороной одну из важных сфер жизни человека – сельское хозяйство. Общеизвестно, что сельское хозяйство в области семеноводства направлено на создание новых сортов растений. А посему в модусе сегодняшнего времени на фоне «снижения зависимости внутреннего рынка от поставок импортной продукции, повышения продовольственной безопасности Российской Федерации» [7] аграрное ведомство нацелено на эволюцию отечественной селекции и семеноводства.

Правительство Российской Федерации своим постановлением от 25.08.2017 № 996 утвердило значимую для аграриев Федеральную научно-техническую программу развития сельского хозяйства на 2017–2030 годы, в ее состав вошли ряд профильных подпрограмм, посвященных развитию селекции в различных областях. Утверждение данной программы является эпохальным событием в сельском хозяйстве.

Таким образом, развитие селекции предрешено аграрной политикой, заложенной в указанной программе. В этой связи можно сделать вывод о том, что высший исполнительный орган власти нацелен на процветание национального сельского хозяйства. И надо сказать, что Минсельхоз России для достижения позитивных результатов в этой области прикладывает большие усилия и слаженно работает с Правительством РФ.

Основная часть. Исторически так сложилось, что российская агропромышленная политика завязана на межгосударственных соглашениях. Поэтому можно встретить в пояснительных записках аграрного ведомства к проектам нормативных правовых актов следующее: «Проект приказа соответствует Договору о Евразийском экономическом союзе от 29 мая 2014 г., а также положениям иных международных договоров Российской Федерации» [8]. Это значит, что от международных актов никуда не деться. Они определяют вектор развития сельского хозяйства. В этой связи национальное законодательство в области семеноводства должно «идти в ногу» с международными соглашениями. Только в этом случае возможен взлет сельского хозяйства и занятие лидирующих позиций.

Коллегия Евразийской экономической комиссии обозначила новые методические подходы к проведению испытаний сортов сельскохозяйственных растений в рамках Евразийского экономического союза. Все это требует переосмысления национального законодательства в области семеноводства и оперативное принятие соответствующих национальных законодательных и норматив-

ных правовых актов. Надо сказать, что Россия в этом направлении достигла внушительных результатов.

Так, с 01.09.2023 вступил в силу Федеральный закон от 30.12.2021 № 454-ФЗ «О семеноводстве». Этот закон долго ждали многие аграрии. Закон сложен из ряда инновационных решений в области семеноводства. Одним из радостных моментов является детальная и полная законодательная регламентация порядка ведения и наполнения Государственного реестра сортов и гибридов сельскохозяйственных растений, допущенных к использованию [3] (далее – Реестр ООС).

В утратившем силу Федеральном законе от 17.12.1997 № 149-ФЗ «О семеноводстве» отсутствовала регламентация указанного реестра, поэтому является правильным решением включить Реестр ООС в ст. 19 Закона.

Вторым перспективным направлением для правоприменителя является законодательная норма ст. 20 Закона, в которой четко регламентируются «испытания и оценка сортов и гибридов сельскохозяйственных растений». Сам Порядок проведения испытаний сортов и гибридов сельскохозяйственных растений по хозяйственно полезным признакам и (или) свойствам сельскохозяйственных растений и форм документов наконец-то утвержден приказом Минсельхоза России от 20.05.2024 № 267. Это большой инновационный прорыв в области семеноводства и слаженная работа Минсельхоза России и ФГБУ «Госсорткомиссия».

Сведения, содержащиеся в Реестре ООС, являются доступными и попадают в публичное пространство на основании п. 4. ст. 19 Закона. А это приводит к контролю и порядку, так как эти данные подлежат отражению на основании ст. 17 Федерального закона от 29.12.2006 № 264-ФЗ «О развитии сельского хозяйства» в специальной системе. Важно, что Минсельхоз России является ее оператором и участником, т. е. он осуществляет цифровизацию и использует соответствующие технологии. Это очень важная и значимая функция в области семеноводства.

Четкая регламентация Реестра ООС в эпоху масштабной цифровизации повысила роль селекции и семеноводства. Так как ст. 19 Закона содержит полную регламентацию указанного реестра, за этот счет произошло обоснованное расширение полномочий Минсельхоза России. Теперь Минсельхоз России формирует, ведет данный реестр и предоставляет сведений из него. Эти полномочия заложены в Положении о Минсельхозе России.

Итогом работы автора сорта сельскохозяйственного растения (селекционер) является создание новых семян и их практическое внедрение в экономический оборот.

Из законодательных норм ГК РФ нам известно, что селекционному достижению предоставляется правовая охрана. Оно регистрируется в Государственном реестре охраняемых селекционных достижений. Ответственным за этот реестр является Минсельхоз России.

Для того чтобы селекционное достижение было зарегистрировано и внесено в указанный реестр, оно, как сказано в ст. 1413 ГК РФ, во-первых, «должно отвечать критериям охраноспособности, как новизна, отличимость, однородность и стабильность». Аналогичные критерии охраноспособности названы в ст.

6 Международной конвенции по охране новых сортов растений, страной-участницей которой является Российская Федерация.

Во-вторых, «селекционное достижение должно относиться к ботаническим родам и видам. Этот перечень устанавливает Минсельхоз России».

Испытание селекционного достижения (нового сорта растений) на отличимость, однородность и стабильность осуществляется по Методике и срокам проведения испытаний селекционного достижения (нового сорта растений) на отличимость, однородность и стабильность, утвержденной приказом Минсельхоза России от 27.10.2020 № 631. Надо сказать, что очень большую и кропотливую работу проделал в этом направлении Минсельхоз России.

Интересно еще одно обстоятельство: до вступления в силу Закона суд дал оценку такому критерию, как «новизна». Так, в судебном решении он указал: «новизну селекционного достижения может опровергнуть лишь факт продажи либо передачи иным образом третьим лицам семян или племенного материала данного селекционного достижения для целей его использования» [10]. Это требует исследования и анализа ст. 1414 ГК РФ.

Исходя из содержания статьи 1413 ГК РФ, «сорт растений будет считаться новым, если на дату подачи заявки на выдачу патента, он не воспроизводился, а семена этого сорта не производились; они не доводились до посевных кондиций для последующего размножения; они не предлагались к продаже и не вводились в гражданский оборот как на территории Российской Федерации ранее чем за один год до указанной даты, так и на территории другого государства ранее чем за четыре года или, если это касается сортов винограда, древесных декоративных, древесных плодовых культур и древесных лесных пород, ранее чем за шесть лет до указанной даты; они не импортировались и не экспортировались в пределах срока, обозначенного в подп. 1.2 п. 3 ст. 1413 ГК РФ; а также в целях, указанных выше, не осуществлялось хранение семян этого сорта».

Следовательно, оценка критерия новизны судебной инстанцией дана неполно. После 2017 года суды воздержались от дачи разъяснения критерию «новизна». В судебных актах можно встретить дублирование нормы из закона, которую зачастую они выдают за авторский текст. А это не направлено на пресечение контрафактных семян и не способствует защите нарушенных или оспоренных прав, а наоборот, девальвирует значимость суда.

Однако следует подробно остановиться на двух действиях «производство» и «воспроизводство».

Из раздела семеноводства известно, что производят только семена (выращивают семена). Это базисное понятие, которым владеют профессионалы в области семеноводства и селекции. Область семеноводства к семенам относит семенной материал, под которым понимается посевной материал, семена, плоды, соплодия и часть сложных плодов, используемых для посева [6. С. 515; 5]. Большое значение имеет понимание такого тезиса, как воспроизводство. Необходимо отметить, что воспроизвести можно только сорт. В Сельскохозяйственном энциклопедическом словаре под «сортом растений» понимается «...разновидность, вид, культивар, совокупность растений, созданная в результате селекции и обладающая определенными, передающимися по наследству мор-

фологическими, физиологическими, хозяйственными признаками и свойствами...» [5; 4].

Производство и воспроизводство – это не синонимы, а два совершенно разных действия. Полезным является понимание такого тезиса, как доведение до посевных кондиций для последующего размножения. К сожалению, суды стирают границы при толковании и прочтении нормы закона. Так, доведение до посевных кондиций для последующего размножения – это подготовка семян к посеву, которая включает в себя в том числе очистку семян от примесей, их сушку (при необходимости), тепловой обогрев, обработку микроэлементами и биологически активными веществами, сортировку и т. д. [5]. Таким образом, довести до посевных кондиций для последующего размножения можно только семенной материал [1. С. 32–35; 2, С. 49–53].

Проведение государственных испытаний селекционных достижений «на отличилось, однородность, стабильность и хозяйственную полезность» осуществляет ФГБУ «Госсорткомиссия» в соответствии с п.п. 3.2.1 и 3.2.2 Устава, утвержденного приказом Минсельхоза России от 18.09.2023 № 741. ФГБУ «Госсорткомиссия» является масштабной фигурой в данном направлении.

Итог государственной регистрации венчается выдачей патента на селекционное достижение. Форма патента утверждена Минсельхозом России. Согласно ст. 1415 ГК РФ, «патент подтверждает приоритет селекционного достижения, авторство и исключительное право на селекционное достижение. Вместе с патентом на селекционное достижение его автору (селекционеру) выдается авторское свидетельство» [2. С. 49–53].

Заключение. В завершение следует отметить, что Закон направлен на пресечение контрафактных семян на внутреннем и международном рынках, а это очень важно в эпоху цифровизации. Насколько данный Закон окажется эффективным покажет время и бесценный опыт селекционеров.

Список литературы

1. Богданова О. В. Права селекционера и их защита // Право и экономика. – 2017. – № 10. – С. 32–35.
2. Богданова О. В. Регистрация селекционного достижения на сорт растений // Право и экономика. – 2018. – № 5. – С. 49–53.
3. Богданова О. В. Цифровизация семеноводства в современном мире // Новые тенденции в развитии современной России в условиях глобализации экономики глазами молодежи: правовые, финансово-экономические и культурно-нравственные аспекты развития: материалы научно-практ. конференции с международным участием. 20 дек. 2021 г., РГСУ, г. Москва. [Электронный ресурс]. – URL: https://conti--group-ru.turbopages.org/turbo/conti--group.ru/s/publ/literatura/cifrovizacija_semenovodstva_v_sovremennom_mire/9-1-0-19213 (дата обращения: 01.09.2024).
4. Общая селекция растений: учебник для вузов / Коновалов Ю. Б., Пыльнев В. В., Хупацария Т. И., Рубец В. С. – СПб., 2013.
5. Растениеводство: учебник / Кузнецова Г. С., Мингалев С. К., Карпухин М. Ю. – Екатеринбург, 2016.

6. Сельскохозяйственный энциклопедический словарь / ред. кол. Н. М. Голышин, В. Г. Гребцова, А. Н. Каштанов [и др.]. – М., 1989.

7. Письмо директора департамента Минсельхоза России от 31.08.2022 № 19/6106 «О семенном материале отечественной селекции» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL:

https://www.consultant.ru/document/cons_doc_LAW_427470/?ysclid=m0e4xq9pq4349369127 (дата обращения: 28.08.2024).

8. Пояснительная записка [Электронный ресурс]. – URL: <https://regulation.gov.ru> (дата обращения: 08.06.2023).

9. Раздел 4 доклада по итогам обобщения правоприменительной практики по осуществлению федерального государственного контроля (надзора) в области семеноводства в отношении семян сельскохозяйственных растений за 2021 год, утвержденный приказом Федеральной службы по ветеринарному и фитосанитарному надзору от 31.03.2022. № 492.

10. Постановление Восемнадцатого арбитражного апелляционного суда от 10.10.2017 № 18АП-9014/2017 по делу № А47-9330/2015 // СПС «КонсультантПлюс» [Электронный ресурс]. – URL:

<https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=RAPS018&n=118624&ysclid=m0e6e3hir1402377536#7U0qlMUpCRreOCr7> (дата обращения: 28.08.2024).

Т. В. Вербицкая,

кандидат политических наук, научный сотрудник,
Государственный архив Свердловской области

ПРОБЛЕМЫ ФОРМИРОВАНИЯ МЕХАНИЗМА ЗАЩИТЫ ОТ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ В ОТНОШЕНИИ ЦИФРОВЫХ КОПИЙ АРХИВНЫХ ДОКУМЕНТОВ, РАЗМЕЩЕННЫХ В СЕТИ ИНТЕРНЕТ

Аннотация. В настоящее время в связи с рассекречиванием архивных документов, возрастанием интереса к изучению истории посредством документальных источников, все больший объем цифровых копий архивных материалов размещается архивными учреждениями в сети Интернет, что обуславливает актуальность проблемы поиска эффективных инструментов защиты от правонарушений в отношении указанных копий. Цель исследования состоит в определении механизма недопущения правообладателем правонарушений (в том числе копирования, распространения) в отношении цифровых копий архивных документов. Установлено, что средства защиты от правонарушений можно подразделить на предварительные (разработка правил пользования цифровыми копиями архивных документов до их размещения на сайте архивного учреждения), текущие (мониторинг, нацеленный на выявление случаев неправомерного использования цифровых копий архивных документов), последующие (привлечение виновных к ответственности). В результате проведения исследования сделан вывод о целесообразности создания единой межархивной системы мониторинга для выявления случаев правонарушений в отно-

шении архивных документов (в том числе их размещения на сторонних Интернет-ресурсах).

Ключевые слова: правовой механизм, система мониторинга, инструменты защиты, исторические источники, культурное наследие, противоправные действия, пресечение правонарушения

PROBLEMS OF FORMING A PROTECTING MECHANISM AGAINST UNLAWFUL ACTIONS TO DIGITAL COPIES OF ARCHIVAL DOCUMENTS POSTED ON THE INTERNET

Abstract. Due to the declassification of archival documents and interest in the study of history through documentary sources, an increasing amount of digital copies of archival materials are placed by archival institutions on the Internet, so it is necessary to find effective tools for protecting against unlawful actions towards these copies. The purpose of the study is to determine the mechanism for preventing the copyright holder from unlawful actions (including copying, distribution) in relation to digital copies of archival documents. It has been established that means of protection against unlawful actions can be divided into preliminary (development of rules for the use of digital copies of archival documents before they are posted on the website of an archival institution), current (monitoring aimed at identifying cases of unlawful use of digital copies of archival documents), subsequent (bringing the perpetrators to responsibility). The author comes to the conclusion that it is advisable to create a unified interarchival monitoring system to identify cases of illegal actions in relation to archival documents (including their placement on third-party Internet resources).

Keywords: legal mechanism, monitoring system, protection tools, historical sources, cultural heritage, illegal actions, suppression of an offense

Введение. Проблемы получения достоверных знаний о различных исторических событиях посредством в том числе изучения документальных источников всегда были значимыми, тем более в условиях, когда рассекречивание различных архивных материалов позволит дополнить имеющиеся знания. Для удобства и помощи исследователям архивные учреждения создают специальные Интернет ресурсы с поисковыми инструментами, на которых размещают цифровые копии архивных документов, в том числе рассекреченных, однако до настоящего времени не было принято законодательных мер, направленных на защиту от неправомерных действий в отношении таких копий, посредством, например, размещения их на сторонних сайтах без согласия правообладателя, с чем уже столкнулись архивные учреждения. Соответственно, не было разработано эффективного механизма правовой защиты правообладателей от подобных неправомерных действий. Для того, чтобы охарактеризовать такой механизм, необходимо прежде всего сформулировать определение цифровой копии архивного документа в качестве объекта защиты.

Основная часть. Следует отметить, что ежегодное изготовление цифровых копий архивных документов является функцией архивов; приоритет в копировании определяется, прежде всего, ценностью документа, его физическим состоянием и заинтересованностью пользователей в изучении конкретного вида

архивных документов (метрических книг, рассекреченных документов). Как отметил И. А. Ключ, «за электронными копиями – большое будущее. И оцифровкой документов должны заниматься именно работники архивов, библиотек и музеев, имеющих представление о фондах своих учреждений и о запросах, как со стороны профессиональных исследователей, так и обычных граждан. Только специалисты могут правильно описать и атрибутировать тот или иной документ» [1. С. 146].

Так, Президентская библиотека имени Б. Н. Ельцина имеет весомый опыт в области каталогизации цифрового контента – формируемый в библиотеке электронный фонд включает в себя цифровые копии библиотечных материалов, архивных документов и музейных предметов, которые объединены в ряд коллекций, в том числе «Память о Великой Победе», «Спорт России», «Кинодокументы»; всего более 800 тыс. записей [5. С. 29].

В специально созданной для хранения цифровых копий базе данных Центрального архива Нижегородской области «Цифровые копии архивных документов» размещено 43 696 документов, в том числе уникальные документы и рукописи из архивных фондов приказных изб конца XVI – начала XVIII в., особо ценные и наиболее востребованные документы из архивных фондов органов государственной власти Нижегородской губернии и Нижнего Новгорода, а также из личных фондов нижегородцев, в том числе фронтовые письма 1941–1945 гг. Общий вес документов составляет 588 Гб [3. С. 65].

Проблемы защиты от неправомерных действий в отношении цифровых копий архивных документов пользуются вниманием ученых [2. С. 42; 4. С. 60; 6. С. 101]. Однако отсутствовало комплексное исследование, позволяющее составить представление о том, каким должен быть эффективный механизм защиты в данной сфере.

Обратимся к определению цифровой копии архивного документа. В п. 2 ст. 3 Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации» [7] содержится определение архивного документа в качестве материального носителя информации, имеющего реквизиты, которые позволяют его идентифицировать и подлежащего хранению в силу значимости этого носителя и информации для личности, общества и государства. Определения цифровой копии архивного документа в указанном законе не содержится. Также не указаны средства защиты правообладателя от неправомерного использования; в ч. 1 ст. 26 данного закона указано, что пользователи имеют право законным образом использовать, передавать, распространять информацию в архивных документах, а также копии архивных документов; в ст. 27 говорится об ответственности за нарушение законодательства об архивном деле. Однако не определены средства защиты правообладателя цифровых копий архивных документов, размещенных в сети Интернет, от их неправомерного использования.

Поскольку в данном законе архивный документ определен в качестве носителя информации, то защита от неправомерных действий в отношении такого документа и его копий может быть обеспечена посредством Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [8]. В п. 11.1 ст. 2 данного Федерального закона содержится определение электронного документа в качестве документированной ин-

формации, представленной в электронной форме – в виде, пригодном для восприятия человеком, с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Цифровую копию архивного документа для целей защиты от неправомерных действий можно определить в качестве специальной разновидности электронного документа, то есть в качестве электронной копии обладающего реквизитами и ценностью для государства, общества личности носителя информации, созданной посредством средств ЭВМ, пригодного для восприятия человека и распространения посредством информационно-телекоммуникационных сетей, и обработки в информационных системах. Соответственно, механизм защиты от неправомерных действий в отношении цифровых копий архивных документов может быть воплощен на основе реализации положений ст. 16 указанного Федерального закона.

Инструменты, которыми наделен правообладатель для защиты от неправомерных действий в указанной сфере на основании ч. 4 ст. 16 указанного федерального закона, можно подразделить на предварительные, текущие и последующие.

К числу предварительных мер можно отнести: предупреждение несанкционированного доступа к информации; предупреждение неблагоприятных последствий нарушения порядка доступа к информации. В качестве текущих мер можно определить своевременное обнаружение фактов неправомерного доступа к информации, недопущение воздействия на технические средства обработки информации, приводящие к тому, что они выходят из строя, контроль за уровнем защищенности информации. Последующие меры – восстановление информации, измененной или уничтоженной из-за неправомерного доступа к ней. По характеру можно выделить такие меры, как наблюдение, контроль и восстановление.

С учетом специфики цифровых копий архивных документов как носителя информации, правообладателем которых является архивное учреждение, к числу предварительных мер можно отнести разработку и размещение на сайте архивного учреждения правил работы с цифровыми копиями архивных документов, а также возможно создание личного кабинета пользователя, через который возможно получение доступа к архивным документам; к числу текущих – внедрение системы мониторинга для выявления случаев появления копий архивных документов на сторонних сайтах без согласия правообладателя; к последующим мерам можно отнести привлечение виновных в неправомерных действиях к ответственности.

Заключение. Таким образом, в связи с тем, что вопросам изучения истории, в том числе по документальным источникам для получения достоверных знаний о тех или иных событиях уделяется все более пристальное внимание, практика размещения архивными учреждениями цифровых копий документов, в том числе рассекреченных, становится все более распространенной, и соответственно, все большую значимость обретает поиск эффективных средств защиты от неправомерного использования таких копий. Для формирования действенного механизма защиты в указанной сфере необходимо в первую очередь включить в законодательство, посвященное защите от неправомерного использования ин-

формации в сети Интернет определения цифровой копии архивного документа в качестве объекта защиты и определить инструменты, посредством которых правообладатель сможет предупредить, пресечь неправомерное использование цифровых копий архивных документов, в том числе разработку правил работы с указанными цифровыми копиями, проставление специального защитного знака, применение системы мониторинга для выявления случаев размещения архивных документов на сторонних Интернет ресурсах без разрешения правообладателя. Наиболее результативной мерой стало бы применение межархивной системы мониторинга для выявления случаев неправомерного использования цифровых копий архивных документов.

Список литературы

1. Ключ И. А. Формы использования цифровых копий архивных документов Государственным архивом административных органов Свердловской области // Вопросы всеобщей истории. – 2022. – № 25. – С. 139–148.
2. Куткин А. В., Назаров А. Н. Оцифровка документов в архивах Российской Федерации: анализ применяемого оборудования и программного обеспечения // Вестник ВНИИДАД. – 2022. – № 6. – С. 41–52.
3. Плотников В. Н. Создание, учет, хранение и использование цифровых копий документов в Центральном архиве Нижегородской области // Отечественные архивы. – 2012. – № 2. – С. 64–65.
4. Селиванова Ю. Г. Интегрированный библиотечный каталог: новая модель представления культурного наследия библиотек, архивов, музеев // Университетская книга. – 2020. – № 3. – С. 58–61.
5. Стегаева М. В. Каталогизация в цифровую эпоху: практика Президентской библиотеки ИМ. Б. Н. Ельцина // Научные и технические библиотеки. – 2020. – № 2. – С. 24–38.
6. Строев С. А. Высоконадежное «вечное» хранение информации: концепция и практические реализации // Репутациология. – 2023. – № 1-2. – С. 69–105.
7. Федеральный закон от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации» // Собрание законодательства Российской Федерации. – 2004. – № 43, ст. 4169.
8. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. – 2006. – № 31 (Часть I), ст. 3448.

Е. Д. Вишнякова,
студент,
Волгоградский государственный аграрный университет
О. В. Кочеткова,
доктор технических наук, профессор
Волгоградский государственный аграрный университет

ИССЛЕДОВАНИЕ ПРОЦЕССА КОНТРОЛЯ РАБОТОСПОСОБНОСТИ ИНТЕГРАЦИИ ДАННЫХ В ДЕЯТЕЛЬНОСТИ СИТУАЦИОННОГО ЦЕНТРА ГУБЕРНАТОРА ВОЛГОГРАДСКОЙ ОБЛАСТИ

Аннотация. Исследование процесса контроля работоспособности интеграции данных из смежных систем в информационно-аналитическую подсистему автоматизированной системы Ситуационного центра Губернатора Волгоградской области для автоматизации процесса. Цель работы определить необходимость автоматизации процесса и выбрать способ реализации проекта. Данная работа является описанием в рамках написания выпускной квалифицированной работы по оптимизации деятельности работников отдела функционирования Ситуационного центра.

Ключевые слова: исследование, цифровые технологии, интеграция данных, ситуационный центр, автоматизация, база данных, аналитика данных, бизнес-аналитика, информационные системы

INVESTIGATION OF THE PROCESS OF MONITORING THE OPERABILITY OF DATA INTEGRATIONS IN THE ACTIVITIES OF THE SITUATIONAL CENTER OF THE GOVERNOR OF THE VOLGOGRAD REGION

Abstract. The study of the process of monitoring the operability of integrating data from related systems into the information and analytical subsystem of the automated system of the Situational Center of the Governor of the Volgograd region to automate the process. The purpose of the research is to determine the need to automate the process and choose a way to implement the project. This research is a description within the framework of writing a graduate qualified work on optimizing the activities of employees of the department of functioning of the Situational Center.

Keywords: research, digital technologies, data integration, situation center, automation, database, data analytics, business analytics, information systems

Введение. На территории Волгоградской области функционирует Ситуационный центр Губернатора Волгоградской области. Его целью является обеспечение своевременного реагирования Губернатора на деятельность региональных и муниципальных структур. Для этого появилась потребность в своде информации в единую базу и представлении аналитики.

Основная часть. В рамках действия Ситуационного центра в 2018 году была разработана автоматизированная система Ситуационного центра Губернатора Волгоградской области.

ИАП АС СЦ ГВО (Подсистема) – это информационно-аналитическая подсистема автоматизированной системы Ситуационного центра Губернатора Волгоградской области.

Главной целью создания Подсистемы была создание инструмента для принятия управленческих решений на уровне региона. Пользователями Подсистемы являются участники межведомственного взаимодействия: главы и сотрудники муниципальных районов региона, руководство региональных государственных структур, глава региона – губернатор Волгоградской области.

Для подключения к Подсистеме необходимо подать запрос в Ситуационный центр. Совместно с сотрудниками СЦ определяются требования к Личному кабинету и данные, которые необходимо мониторить. Более подробно показано на диаграмме eEPC (рис. 1).

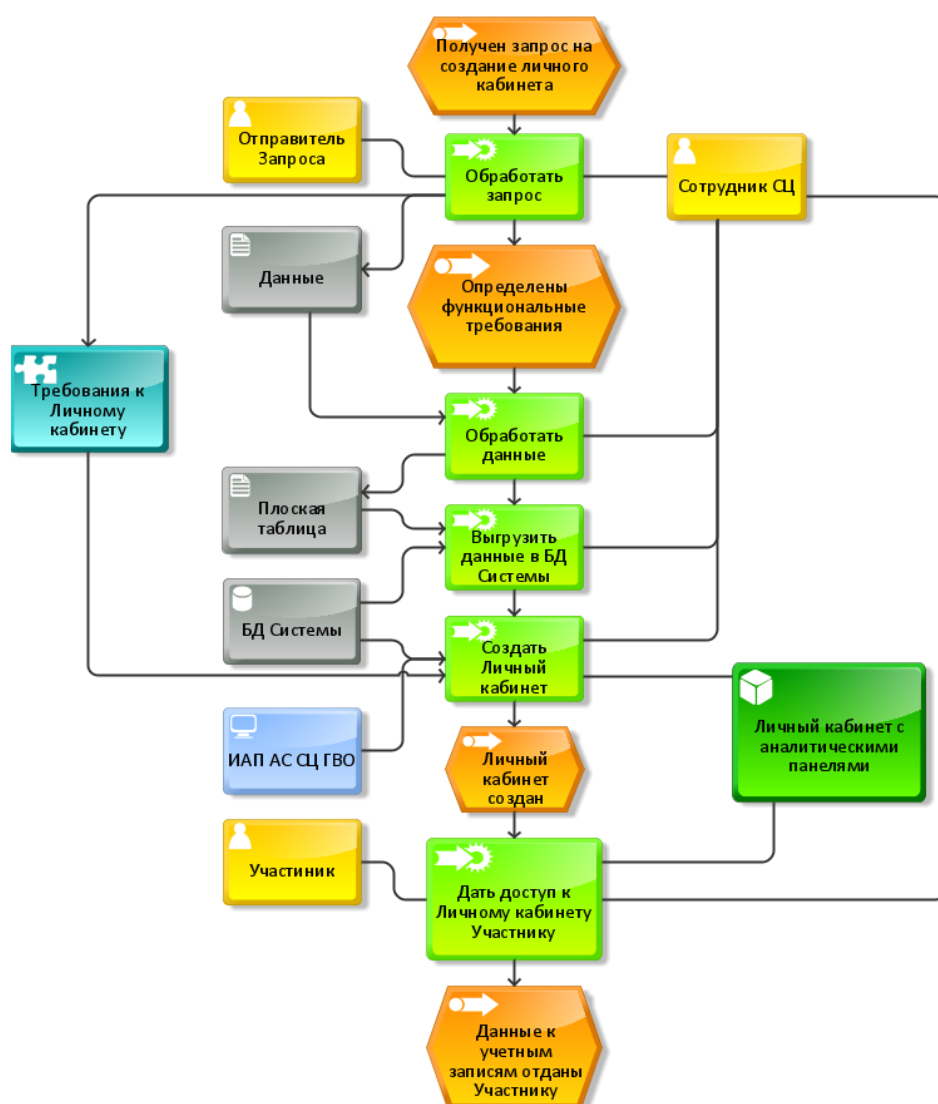


Рис. 1. eEPC-диаграмма создания Личного кабинета Участника

Подсистема включает в себя несколько функциональных модулей (компонентов), каждый из которых решает свои задачи.

Одним из важных модулей для ИАП АС СЦ ГВО является «Компонент сбора, хранения и управления данными». С его помощью загружают данные в БД Подсистемы. В Подсистеме используется три вида ввода данных: «ручной», с помощью ETL и интеграция. При «ручном» виде загрузки, при создании виджета. ETL загрузчик выгружает данные из файла с ПК пользователя. Интеграцию используют при выгрузке данных напрямую из другой системы.

Участники могут запросить настройку интеграции данных из систем региональных и федеральных уровней. На текущий момент реализовано 22 интеграции со сторонними системами.

В работе будет изучен способ получения данных через автоматизированное интегрирование их прямо в Подсистему. Поэтому рассмотрим процесс получения данных и его достоинства и недостатки (рис. 2).

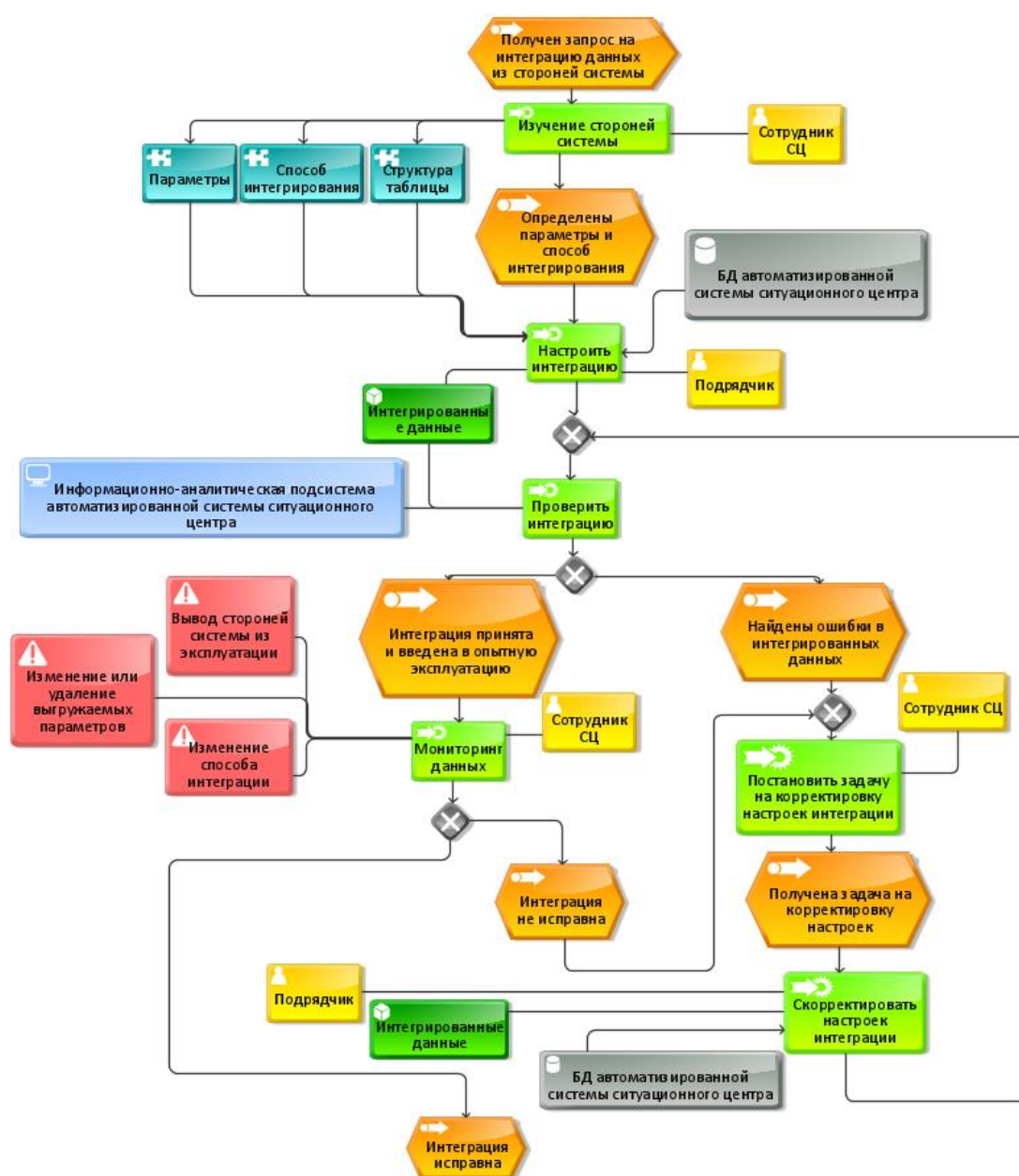


Рис. 2. eEPC-диаграмма процесса настройки интеграции

Настройка интеграции – сложный процесс, при котором сотрудники ситуационного центра привлекают сторонних специалистов (подрядчиков). При составлении заявки на настройку интеграции сотрудники ситуационного центра в адрес подрядчика должны направить:

- параметры, которые необходимо выгружать из сторонней системы. Зависит от запросов пользователей;
- структуры таблиц (таблицы). Зависит от параметров;
- способ интегрирования. Зависит от возможностей сторонней системы и ИАП АС СЦ ГВО.

После определения параметров, способа интеграции и структур таблиц, сотрудники СЦ передают их подрядчикам, для настройки. В среднем весь процесс настройки интеграции занимает от нескольких дней до месяца. Сама проверка работоспособности интеграций занимает от 1 до 3 дней.

Из-за постоянного развития и усовершенствования технологий передачи данные риски могут возникнуть как во время эксплуатации интеграции, так и при первой ее настройке. Что негативно сказывается на уровне удовлетворенности пользователей и их доверии Подсистеме.

Поэтому для сокращения времени проверки и реагирования на появившиеся риски, а также исключения человеческого фактора при проверке, что увеличивает качество, было принято решение использовать инструмент для проверки работоспособности интеграций. Чтобы подобрать подходящий инструмент, необходимо определить и разобрать критерии, по которым необходимо сделать выбор, изучим подробнее процесс.

Исходя из этого, выдвигаем гипотезу: если разработать инструмент для проверки работоспособности интеграций, то количество времени на проверку и риски сбоев сократятся.

Чтоб автоматизировать механизм контроля необходимо:

- изучить данных уже действующих интеграций;
- разработать метод проверки;
- создать скрипт;
- проанализировать эффективность автоматизации.

Все эти этапы можно реализовать с минимумом затрат:

1) для выгрузки данных использовать SQL-запросы к БД. ПО можно использовать любое, подходящее для этого;

2) изучить подробно часто возникающие ошибки и составить правила проверки. Для этого необходимо изучить соответствующую литературу;

3) разработать скрипт, который будет проверять данные, выявлять ошибки и оповещать о них. Использовать можно любой текстовый редактор и язык программирования;

4) изучить показатели до применения разработок и после. Основные показатели будут время и качество проверки.

Целью исследования является повышение качество контроля за работоспособностью интеграций, а также сокращение временных издержек на проведение проверки данных.

Объектом работы будет информационно-аналитическая подсистема автоматизированной системы Ситуационного центра Губернатора Волгоградской области.

Предмет работы: механизм контроля работоспособности интеграции.

Для достижения цели необходимо поставить и решить следующие задачи:

- 1) изучить предметную область;
- 2) определить инструменты для реализации проекта;
- 3) разработать автоматизированный механизм контроля;
- 4) оценить эффективность использования инструмента для проверки работоспособности интеграций деятельности ИАП АС СЦ ГВО.

Использование инструмента должно максимизировать эффективность использования автоматизированных интеграций и снизить риски сбоев для принимающей стороны процесса.

Сотрудники СЦ при использовании данной разработки смогут ставить детализированные задачи на решение проблем, возникших при использовании интеграций, так как будут знать причину сбоя или ошибки.

Выбор объекта исследования и сбор материалов об объекте исследования. Чтобы достичь цели работы, необходимо изучить принцип проверки интеграций. Из этого следует, что процесс передачи данных будет объектом исследования.

Интеграция данных – это набор методов, инструментов и архитектурных процедур, позволяющих компаниям комбинировать и использовать все типы данных. Процесс интеграции обеспечивает не только консолидацию, но и чистоту данных, а также отсутствие ошибок, что позволяет бизнесу использовать данные максимально эффективно [8].

Изучим историю интеграций данных: предпосылки их создания, актуальность использования и их проблематику.

Преимущества и риски использования интегрирования данных. Объединение данных из разных источников стоит на повестке дня с тех пор, как бизнес-системы начали собирать данные. Лишь в начале 1980-х годов ученые-информатики начали проектировать системы, поддерживающие совместимость неоднородных и отдельных баз данных [13]

В 1991 году была запущена первая система интеграции данных в Университете штата Миннесота. Перед университетом стояла задача обеспечить совместимость тысяч баз данных о населении. Система собирала и организовывала данные из разрозненных источников, преобразовывала их и загружала в единую схему ракурсов.

При долговременном использовании системы возникали различные проблемы, связанные с качеством данных, управлением, моделированием, с изоляцией и разрозненностью данных.

Проблема интеграции данных является неотъемлемым аспектом проблематики развития информационной инфраструктуры предприятия. То есть, если развивается инфраструктура источников интеграции, то и процесс интегрирования данных должен развиваться.

Если рассмотреть процесс интеграции со стороны бизнеса-процесса, как в статье электронного журнала DataRevie, можно выделить три преимущества использования интеграции данных [9]:

- стандартизация. Интеграция данных позволяет выбрать и установить единый стандарт представления и работы с данными, что значительно упрощает взаимодействие и ускоряет процесс передачи данных;
- автоматизация. Интеграция данных предполагает автоматический сбор информации из разрозненных источников в режиме реального времени и их моментальное преобразование в предустановленный формат;
- эффективность. Интеграция данных значительно повышает эффективность принятия управленческих решений. Так как данные собираются и преобразовываются в режиме реального времени, то пользователь может принимать управленческие решения в любое время, без ожидания.

То есть использование интеграция уменьшает время на сбор данных и повышает эффективность их использования в бизнес-процессах. Для деятельности СЦ это важно для достижения ее главной цели: своевременного реагирования Губернатора на деятельность региональных и муниципальных структур.

Для определения важности интегрирования данных для Подсистемы, рассмотрим причины ее использования. IT-компания Deco System, в своем блоге выделяют четыре причины использования интеграции данных в ИС [11]:

- Обеспечение единого доступа к данным. Интеграция позволяет обеспечить согласованность данных, делая их доступными.
- Улучшение взаимодействия между подразделениями или организациями. Когда системы интегрированы, команды могут быстрее и эффективнее сотрудничать.
- Повышение эффективности и экономии ресурсов. Упрощение процессов, уменьшение ручного труда. Это, в свою очередь, ведет к сокращению затрат и ошибок.
- Гибкость и адаптивность к изменениям. Легкая модификация в ответ на изменение требований и технологические инновации.

Из этого следует, что интегрирование данных наилучший способ для загрузки данных в базу данных BI-системы, которое необходимо развивать.

Типы интеграций и технологии реализации. Существует три типа интеграций: консолидация, федерализация и распространение (рис. 3) [10].

Консолидация данных подразумевает сбор данных из нескольких первичных источников в одно постоянное место хранения.

Консолидация имеет задержку между обновлением информации в источнике, и обновленные данные появляются в конечном месте хранения. Задержка может занимать от нескольких секунд до нескольких дней. Время задержки зависит от настроек обновления данных в источнике и конечном месте хранения и параметров передачи данных.

Федерализация данных преобразует данные из одного или нескольких источников в единую виртуальную картину. Преобразование происходит по запросу к виртуальной картине, который запускает процесс извлечение данных из источников.

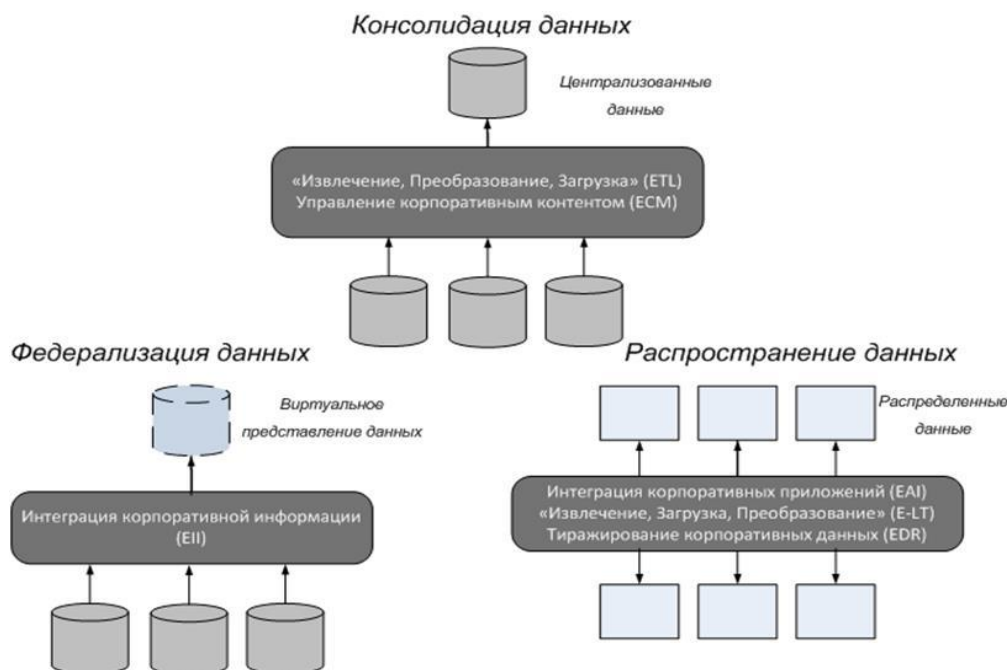


Рис. 3. Типы интеграций

Метод преобразования данных из одного или нескольких источников по запросу называется федерализацией данных. Запрос, который преобразует данные, запускает процесс передачи данных.

Необходимо отметить, что в англоязычной литературе термин *federated data warehouse* сейчас используется в двух разных значениях. Часть специалистов подразумевает под федеративным хранилищем создание виртуальной структуры, оперирующей с выборками данных. Другие называют федеративным хранилищем единый физический репозиторий, работающий с копиями данных, который, другими словами, может быть назван распределенным хранилищем.

Метод копирования данных из источников в несколько мест, называется распространением данных. Главными преимуществами распространения данных являются передача данных в режиме реального времени и гарантированная доставка данных.

Существует несколько техник, которые используются в настройке интеграций [12]:

1. ETL (*extract, transform, load* – «извлечение, трансформация, загрузка») – заключается в извлечении данных, преобразовании их в нужный формат и загрузке в целевую систему.

2. ELT (*extract, load, transform* – «извлечение, загрузка, трансформация») – заключается в извлечении данных и преобразовании их в нужный формат только после загрузки в целевую систему.

3. *Data virtualization* – данные остаются у источников, но представлены в виде единой виртуальной таблицы.

При интегрировании данных в базу данных Подсистемы СЦ используют консолидацию данных в технике ETL. При этом данные копируются из сторонней системы в ИАП, а не удаляются. Но копируются не все данные, а только не-

обходимые, которые указаны сотрудниками СЦ. По их же требованиям и происходит трансформация или преобразование данных до выгрузки их в базу данных

Изучим преимущества консолидации данных и технологии ETL. Консолидация данных может повысить качество передачи данных из других систем. Данные сразу копируются в базу Подсистемы, что обеспечивает доступ к ним и упрощает их управление. При необходимости внесение корректировок или запроса дополнительных манипуляций с данными нет необходимости повторного обращения к персоналу сторонней системы. Вместо этого можно просто расширить диапазон запрашиваемых данных через кодирование. За счет закрытости базы и единого контроля обеспечивается безопасность данных. Так Подсистема исключает распространение данных между Участниками без их согласия.

Рассмотрим этапы процесса ETL: извлечение, трансформация и загрузка. Извлечение: система собирает данные из целевых источников, например, API-интерфейсов, датчиков, баз данных, серверных журналов JSON, маркетинговых инструментов и так далее.

Какие могут быть источники:

- базы данных и системы;
- различные среды;
- приложения;
- CRM-системы;
- платформы хранения данных;
- хранилища данных;
- инструменты аналитики.

Для преобразования данные проходят через анализ, разделение/объединение и фильтрацию. После преобразования отправляются в конечную точку и проходят очередную обработку. Поэтому чаще используют форматы JSON, Parquet или CSV для хранения данных.

Запрашиваемые данные не всегда подходят для хранения в целевой системе в том же виде, что и в источнике, поэтому некоторые из них требуют преобразования. Преобразование включает в себя:

- очистку данных, которая убирает дубликаты, заменяет или удаляет нулевых значений, ищет и исправляет ошибки;
- разделение помогает делить данные из одной ячейки на несколько;
- извлечение позволяет достать отдельную информацию из поля данных;
- объединение данных из нескольких ячеек в одну.

После преобразованная информация из промежуточной области отправляется в целевую базу данных, озеро данных или хранилище данных. При этом можно использовать полную загрузку или добавочную. Полная загрузка – выгрузка всех данных из источника чаще используется для исследований. Полная загрузка может длиться долгое время и нуждается в больших вычислительных ресурсах. Добавочная загрузка сравнивает входные данные с уже имеющимися и создает новые записи только в случае появления новых данных в источниках.

Методы проверки данных. Наличие рисков предусматривает управление ими. Так как ИАП является объектом, на который направленно исследование, то необходимо проводить проверку данных, лежащих в базе данных Подсистемы.

Проверка данных – это процесс обеспечения точности, полноты и согласованности данных, собранных, хранящихся и анализируемых предприятием. Существует несколько методов проверки данных. Проверка типа данных проверяет, находятся ли данные в ячейке и имеют ли соответствующий тип. Проверка кода гарантирует, что поля выбраны из представленного списка и соответствуют стандартам форматирования. Подходит данным, у которых есть определенный список, например, индекс адреса или наименование субъектов.

Проверка диапазона позволяет оценить, соответствуют ли входные данные диапазону. Например, для геоданных, ограниченных областью или субъектом РФ.

Проверка формата. Проверка соответствия необходимого формата данных в выбранном типе данных. Если формат даты определен в виде ДД.ММ.ГГГГ, то он должен соответствовать ему.

Проверка присутствия гарантирует наличие данных в ячейках.

Проверка длины проверяет, что в ячейке находятся необходимое количество символов.

Так как данные требующие проверки являются разнотипными и разноформатными, то при разработке инструмента проверки необходимо применение комплекса методов. Из представленных методов выделяют основные факторы проверки: формат; диапазон; завершенность; согласованность; зависимость атрибута; недействительные значения; отсутствующие значения; орфографические ошибки.

Проверка данных можно провести одним из трех способов: сценарии, корпоративные инструменты и инструменты с открытым исходным кодом. Выбор и использование правильных инструментов и инфраструктур проверки данных может оказать существенное влияние на потенциал Подсистемы, потому что могут помочь достичь следующих преимуществ.

Повышение качества и надежности данных. Инструменты и системы проверки могут гарантировать точность данных и их полноту. Это в свою очередь сказывается на качестве работы всей Подсистемы и удовлетворенности пользователей.

Повышение безопасности и соответствия требованиям. Использование специализированного инструментария в процессе проверки защищает данные от нежелательных действий персонала, а также обеспечивает соответствия данных требованиям сотрудников СЦ.

Оптимизация производительности и эффективности данных. Оптимизация скорости, масштабируемость и экономическая эффективность операций с данными сказывается на работоспособности всей Подсистемы и отдела СЦ в частности.

При выборе инструментария для проверки данных стоит обратить внимание на некоторые аспекты:

1. Тип и сложность данных. Для разных типов данных и источников могут потребоваться разные методы и сценарии проверки.

2. Объем и частота проверки данных могут повлиять на выбор и использование инструментов и инфраструктур проверки данных, поскольку некоторые инструменты могут быть более подходящими для пакетной проверки, тогда как другие могут быть более подходящими для проверки в режиме реального времени или потоковой проверки.

3. Уровень и режим проверки данных определяют, насколько глубокой и интерактивной является проверка данных. Это может зависеть от целей проверки данных, критериев проверки данных и методов проверки данных.

Проверка данных – это не только технический процесс, но и стратегический, который обеспечивает качество, точность и согласованность данных. Получение ценной информации способствует своевременной оптимизации операций и улучшает качество использования Подсистемы.

Процесс проверки включает в себя проверку данных на соответствие заранее определенным правилам или критериям, а также выявление и исправление любых ошибок или несоответствий. Проверка данных может помочь избежать распространенных ошибок, таких как пропущенные значения, опечатки, дубликаты, выбросы или недопустимые форматы. Это также может помочь оптимизировать процесс интеграции данных и принятия решений, предоставляя чистые, последовательные и актуальные данные.

В зависимости от типа, источника и цели ваших данных вам может потребоваться применить различные методы в процессе проверки данных. А для улучшения процесса проверки данных необходимо:

1. Четкое и последовательное определение правил и критериев проверки данных.

2. Выбор подходящего уровня и метода проверки данных. Проверка данных может выполняться на разных уровнях, таких как уровень поля, записи, файла или базы данных. Это также может быть сделано с использованием различных методов, таких как ручной, автоматический или полуавтоматический.

3. Использование подходящих инструментов и методов для проверки данных. Для проверки данных доступно множество инструментов и методов, таких как программное обеспечение для обеспечения качества данных, профилирование данных, очистка данных, преобразование данных, проверка данных и сверка данных.

4. Тестирование и контроль процесса проверки данных. Перед внедрением использования инструментария на постоянную основу необходимо протестировать и оценить его эффективность.

Анализ предметной области в рамках поставленной задачи по материалам научно-технических зарубежных публикаций и информации в сети Интернет. Инструменты по проверке данных внедрены в некоторые платформы по управлению данными. Но их использование невозможно из-за условий контрактов о развитии Системы.

При составлении контракта о создании и контрактов о развитие и сопровождении Подсистемы прописано условие, исключающее подключение сторонних ПО для функционирования Подсистемы. Этот пункт обеспечивает целостность автоматизированной системы, ее самостоятельность и независимость

в функционировании. А также данный пункт обеспечивает повышенную конфиденциальность данных, которые выгружают в базу данных Подсистемы.

Из этого следует, что сотрудникам СЦ подойдет способ реализации проверки «сценарий». То есть код, который будет проводить проверку данных.

При поиске в сети Интернет, представляются отрывки и примеры анализа небольших данных, а также теория о тестировании баз данных. Но в предложенных множествах ссылок на различные сайты, не было найдено какого-либо готового решения подходящего данных Подсистемы. Например, в статье о скриптах описаны основы тестирования данных и примеры сценариев кода для проверки небольших данных. Также Интернете можно найти и теорию по тестированию базы данных. Но вся информация дана для изучения, и практических работ, которые можно сразу применить, нет.

Обратимся к зарубежным источникам. Так в поисковой системе Google будем искать «data validation» и «the process of data validation», но в зарубежных источниках тоже приведена только теории. При этом информация, которая представлена в зарубежных источниках, дублируется и в российских. Все источники располагают общей информацией и общими примерами. В списке используемых источников они под номерами 2–6 и 8, 9, 12. Из этого следует, что, используя собранную информацию, мы можем разработать продукт, подходящий под характеристики данных Подсистемы.

Работа по исследованию данных в деятельности ИАП является уникальной за счет специфики объекта исследования. Системы подобные ИАП АС СЦ ГВО невозможно встретить, так как она разрабатывалась по запросам и требованиям Волгоградской области и является интеллектуальной собственностью. Поэтому тема исследования является уникальной и актуальной.

Создание схемы бизнес-процесса. Для более детального изучения проблематики работы необходимо рассмотреть подробно сам бизнес-процесс. Схема бизнес-процессов будет основана на eEPC-диаграмме процесса настройки интеграции (рис. 2). Действующие роли для схемы: Сотрудник СЦ, Пользователь и Подрядчик. А переменными будут: требования и корректность работоспособности интеграции. Формат для требований определим как файл, а для определения корректности – как строка.

После определения ролей и переменных – создание диаграммы в нотации BPWN. В итоге получаем схему, изображенную на рис. 4.

Составим формы для процессов «Сформировать требования к интеграции», «Настройка интеграции», «Проверка интеграции» и «Мониторинг работоспособности интеграции».

Результат процесса «Сформировать требования к процессу интеграции» – это сформированный файл требований. Поэтому в форме необходимо предусмотреть отправку файла от Сотрудника СЦ Подрядчику (рис. 5).

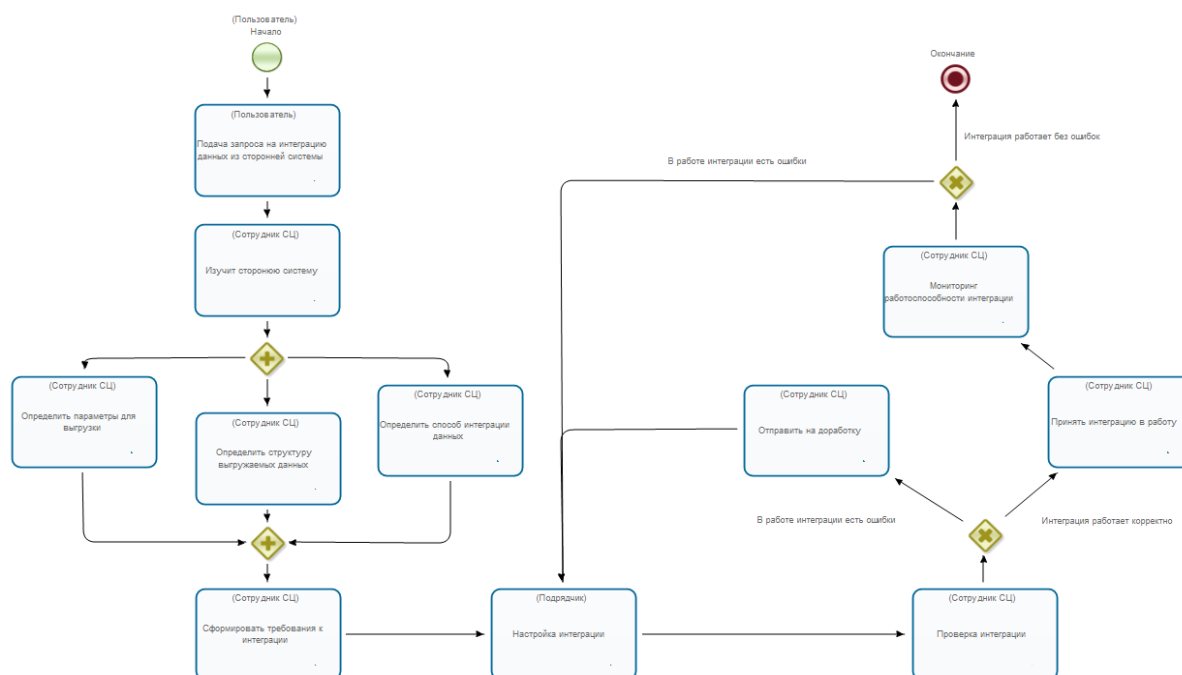


Рис. 4. BPWN-диаграмма процесса настройки интеграции

Рис. 5. Форма «Сформировать требования к интеграции»

Чтобы подрядчик смог получить информацию, необходимо в форме предусмотреть возможность скачать файл с требованиями. Поэтому форма показана на рис. 6.

Рис. 6. Форма «Настройка интеграции»

Форма для «Проверка интеграции» (рис. 7) должна показать корректность работы интеграции. Поэтому используя переменную «корректность работоспособности интеграции» и в форме назначим ей значение «да» или «нет». От ответа будет зависеть следующий процесс. Если интеграция работает корректно, то Сотрудник СЦ принимает интеграцию в работу или же отправляет на доработку.

Рис. 7. Форма «Проверка интеграции»

Соответствующую форму необходимо настроить для процесса «Мониторинг работоспособности интеграции» (рис. 8). Только если интеграция работает без ошибок, весь процесс проверки работоспособности завершается или интеграция снова отправляется на доработку.

Рис. 8. Форма «Мониторинг работоспособности интеграции»

Заведение учетных записей и создание отношений. Для создания учетных записей для соответствующих ролей, откроем веб-интерфейс RupaWFE и зайдем под администратором. Перейдя во вкладку «Исполнители» и заводим пользователей «Сотрудник СЦ», «Пользователь» и «Подрядчик». Для удобства соберем их в одну группу «Проверка работоспособности интеграций» (рис. 9).

Для загрузки созданного процесса (рис. 4) в веб-интерфейс переходим во вкладку «Запустить процесс» и разворачиваем «Загрузить определение процесса». Выбрав выгруженный процесс, нажимаем на «Загрузить определение процесса» (рис. 10).

Свойства исполнителя		Задачи сотрудников группы	Обладатели полномочий
Имя	Проверка работоспособности интеграций *		
Описание			
Группа LDAP			
Применить			

Группы исполнителя	
Вид	Без фильтра
Добавить	
☐	Имя / Описание
Удалить	

Члены группы			
Вид: Без фильтра			
Добавить			
☐	Имя /	Полное Имя	Описание
☐	Подрядчик		
☐	Пользователь		
☐	Сотрудник СЦ		
Всего: 3			
Удалить			

Отношения, в которые исполнитель входит в правой части	
Имя отношения	Описание

Отношения, в которые исполнитель входит в левой части	
Имя отношения	Описание

Рис. 9. Исполнители по процессу «Проверка работоспособности интеграций»

Меню	Определения процессов																								
- Список заданий Запустить процесс - Запущенные процессы - Архивные процессы - Исполнители - Отчёты - Отношения - Бот станции - Источники данных - Внутреннее хранилище - Система - Ошибки - Настройки - Логи сервера - Задания сотрудников - Отправить сигнал	Вид: Без фильтра Загрузить определение процесса Определение процесса Настройка интеграции.par - 44 Kb Тип процесса Создать новый тип Дней до архивации (пусто = по умолчанию) Применить тип ☒ Только к новым процессам ☐ Ко всем процессам Загрузить определение процесса История <table border="1"> <thead> <tr> <th>☐</th> <th>Запустить</th> <th>Имя /</th> <th>Описание</th> <th>Тип процесса</th> <th>Дата загр</th> </tr> </thead> <tbody> <tr> <td>☐</td> <td></td> <td>AjaxFormDemo</td> <td>AJAX support demo</td> <td>Other</td> <td>14.11.2021</td> </tr> <tr> <td>☐</td> <td></td> <td>BotDemo</td> <td>Bot demo process (no start form provided)</td> <td>Bots</td> <td>14.11.2021</td> </tr> <tr> <td>☐</td> <td></td> <td>Business...</td> <td>Participants of this process are members of manager...</td> <td>Company</td> <td>14.11.2021</td> </tr> </tbody> </table>	☐	Запустить	Имя /	Описание	Тип процесса	Дата загр	☐		AjaxFormDemo	AJAX support demo	Other	14.11.2021	☐		BotDemo	Bot demo process (no start form provided)	Bots	14.11.2021	☐		Business...	Participants of this process are members of manager...	Company	14.11.2021
☐	Запустить	Имя /	Описание	Тип процесса	Дата загр																				
☐		AjaxFormDemo	AJAX support demo	Other	14.11.2021																				
☐		BotDemo	Bot demo process (no start form provided)	Bots	14.11.2021																				
☐		Business...	Participants of this process are members of manager...	Company	14.11.2021																				

Рис. 10. Загрузка процесса в веб-интерфейс RunaWFE

Потом нажимаем на новый процесс и переходим во вкладку «Запущенные процессы» и открываем процесс для назначения исполнителей. В блоке «Роли процесса» назначаем ролям соответствующих исполнителей (рис. 11).

Роли процесса			
Изменить исполнителя			
Имя	Глобальная	Исполнитель	О
Сотрудник СЦ		Сотрудник СЦ	3+
Пользователь		Пользователь	3+
Подрядчик		Подрядчик	3+
Переманить процесс			

Рис. 11. Назначенные исполнители на соответствующие роли

Организация тестирования и реализация цикла тестирования. Для тестирования заходим под учетной записью Пользователя и завершаем задачу «Поддача запроса на интеграцию данных из сторонней системы» (рис. 12).

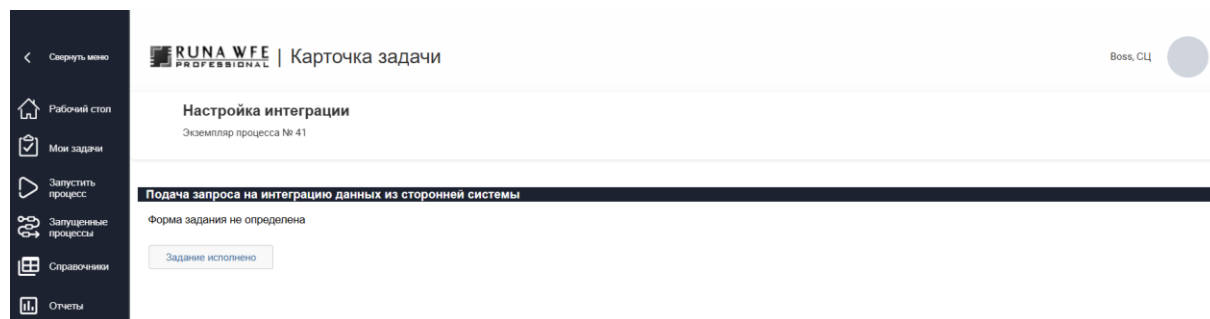


Рис. 12. Выполнение задачи «Поддача запроса на интеграцию данных из сторонней системы»

Дальше заходим под Сотрудником СЦ и выполняем поочередно задачи:

- 1) изучить стороннюю систему;
- 2) определить способ интеграции данных;
- 3) определить параметры для загрузки;
- 4) определить структуру выгружаемых данных;

Определение проблематики. Как видно из моделирования процесса настройки: процесс в данном виде несовершенен. Отсутствие контроля над данными приводят к их потере и отказу передачи, что приводит к недействительным показателям для показа пользователю. Такие показатели влияют на принятие решений на уровне регионального управления.

Выбор методов и инструментария исследования. Перед созданием самого инструмента, который будет контролировать потоки данных, необходимо определить на каком языке будет он создан. Для этого был проведен анализ нескольких вариантов.

Существует еще множество языков, которые можно включить в этот список. Но наш выбор был сделан исходя из функциональных возможностей оборудования и специализации экспертов.

В СЦ уже используется несколько разработок на Python, поэтому для его использования уже все подключено к местам сотрудников. SQL – уникальный язык, который тоже используется в работе сотрудников, поэтому был включен в список. Java использовался в создании и развитии многих модулей Подсистемы, поэтому подрядчики рекомендовали рассмотреть его вариант. Matlab используется в многих научных сферах, а также позволяет использовать сложные математические вычисления.

Python – популярный язык программирования общего назначения и широко используется в сообществе специалистов по данным. SQL (язык структурированных запросов) определяет, управляет и запрашивает реляционные базы данных. Со временем язык потерпел множество видоизменений, но основные его принципы остаются неизменными. Java – популярный язык общего назначения,

который работает на виртуальной машине Java Virtual Machine. Это абстрактная вычислительная система, которая обеспечивает плавную переносимость между платформами. Matlab – это признанный язык для численных расчетов, используемый как в научных целях, так и в индустрии. Он был разработан и лицензирован MathWorks, компанией, созданной в 1984 году, основной целью которой являлось коммерциализация программного обеспечения.

Изучим подробнее варианты перед проведением исследования. Для этого составим таблицу (табл. 1) с описанием их преимуществ, недостатков, доступности и комментарии специалистов и экспертов.

Таблица 1

Характеристики вариантов для проведения исследования

Вариант	Преимущества	Недостатки	Доступность	Комментарий
Python	Python – универсальный инструмент. Он был задуман как язык, который можно легко расширять, дописывая собственные модули и функции. Он может выполнять одни и те же действия на различных операционных системах без переписывания программ под них. Если раньше для работы с графикой, разными форматами файлов, системными и сторонними библиотеками требовалось изменение кода и модели программирования, то с Python эта необходимость отпадает. Одно из главных преимуществ языка – низкий порог входа. Отсюда и большое сообщество питонистов, которое, если что, всегда поможет с вопросами. Один из главных недостатков – это высокоуровневый язык, поэтому у программирования на нем есть ограничения, например, по	Производительность. Здесь Python проигрывает таким языкам, как C или C++, которые обычно используются для системного программирования и создания высокопроизводительных приложений. Мобильные приложения. В разработке мобильных приложений Python используется не так часто, как Java, Swift или Kotlin. Существуют библиотеки для создания мобильных приложений на Python, например, Kivy, но широкого распространения в разработке они не нашли. Не компилируется в машинный код. Это делает Python более универсальным, но в то же время снижает производительность по сравнению с кодом, написанным на компилируемом языке [16]	Бесплатная лицензия Для использования подходят множества редакторов	Python является хорошим вариантом для целей науки о данных (data science), и это утверждение справедливо как для начального, так и для продвинутого уровней работы в данной области. Большая часть науки о данных сосредоточена вокруг процесса ETL (извлечение-преобразование-загрузка). Эта особенность делает Python идеально подходящим для таких целей языком программирования. Библиотеки, такие как Tensorflow от Google, делают Python очень интересным языком для работы в области машинного обучения [23]

Вариант	Преимущества	Недостатки	Доступность	Комментарий
	доступу к оперативной памяти или процессору [16]			
SQL	Стандартизация. Разработанные международные нормы позволяют унифицировать базы данных, построенные на реляционной модели Реляционная основа. Табличная структура интерфейса облегчает пользователям работу с БД Можно создавать интерактивные запросы. Пользователю доступно все содержимое массива в реальном времени Простая интеграция на программном уровне. Приложения, которые используют доступ к БД, легко программируются с помощью языка SQL Гибкость настроек. Разработчик может динамически изменять, расширять структуру базы, настраивая ее под конкретные параметры Универсальность. Работать с языком могут специалисты разного профиля: разработчики БД, администраторы, программисты и конечные пользователи [9]	Не является на 100% реляционным. Эдгар Франк Кодд и Крис Дейт, создавшие реляционную модель, нашли несколько системных дефектов в синтаксисе языка. Это выражается в повторяющихся строках, неопределенных значениях, высокой избыточности и других отступлениях от канонов Сложность в освоении. Изначально среда создавалась как простой и понятный инструмент. Со временем язык эволюционировал и стал настолько сложным, что перешел в категорию инструментов для программистов Проблемы с совместимостью. Старые версии не поддерживают древовидные иерархические структуры, которые есть во многих современных БД [9]	Лицензия платная и бесплатная	SQL более полезен в качестве языка для обработки данных, чем в качестве периферийного аналитического инструмента. Тем не менее, так много процессов в области науки о данных зависит от ETL, а долговечность и эффективность SQL лишней раз свидетельствуют о том, что такой ЯП должен знать каждый специалист по данным (data scientist)

Вариант	Преимущества	Недостатки	Доступность	Комментарий
Java	С-подобный синтаксис – негласный стандарт среди программистов. Синтаксис Java основан на C++, но упрощен, что позволяет новичкам быстрее учиться и эффективнее использовать код. Возможности объектно-ориентированного программирования. ООП позволяет создавать расширяемые системы (extensible systems), которые заставляют работать систему с новыми компонентами без внесения изменений. Статическая типизация – заблаговременное объявление типа переменных, которое не может быть изменено впоследствии. Благодаря ей ошибок можно избежать уже на первых этапах. Java ориентирована на JVM (Java Virtual Machine). Эта программа позволяет запускать написанный на Java код на любом поддерживаемом устройстве или операционной системе. Помогает и обратная совместимость: при переходе на новую версию JVM разработчикам не нужно менять старый код. Большое сообщество. На GitHub свыше 128 тысяч публичных репозиторий с Java-проектами [15]	Кроссплатформенность. С одной стороны, она позволяет разрабатывать приложения одновременно под различные системы: Windows, Linux, MacOS, – но при этом приходится подстраиваться под ранние версии Java, чтобы сохранить работоспособность на устройствах предыдущих поколений. Строгость языка. Она позволяет четко понимать, что выполняет написанный код, но при этом может стать препятствием в изучении языка новичками [15]		Много чего можно сказать в пользу изучения Java как языка для работы в области науки о данных. Многие компании оценят возможность беспрепятственной интеграции готового кода программного продукта в собственную кодовую базу, а производительность и типобезопасность Java являются его неоспоримыми преимуществами. Тем не менее, к недостаткам такого языка можно отнести тот факт, что у него отсутствуют наборы специфических пакетов, которые доступны для других языков. Несмотря на такой недостаток, Java является языком программирования, которому обязательно стоит уделить внимание, особенно если вы уже знаете R или Python.

Вариант	Преимущества	Недостатки	Доступность	Комментарий
MATLAB	Широкий функционал. Язык MatLab включает продвинутую библиотеку для обработки и построения графиков, интегрированные функции линейной алгебры (LAPACK, BLAS), быстрого преобразования Фурье (FFTW), работы с полиномами, базовой статистики, решения дифференциальных уравнений и пр. Обновляемость. Основные обновления языка и всей среды программирования происходят два раза в год. Преобразования в «быстрый» код. Программы, написанные на MatLab, можно перевести на C/C++ с помощью MatLab Coder. Интегрированность. Большой выбор прикладных приложений от официальных и сторонних разработчиков расширяет возможности языка. Большое научное сообщество. Язык MatLab используется во многих университетах и исследовательских институтах [4]	Перегруженность. Большое число команд и операторов существенно замедляют работу программ, написанных на MatLab (в последних версиях этот недостаток практически устранен). Данные хранятся в оперативной памяти в виде векторов, поэтому на быстрое действие также сильно влияет скорость векторизации – преобразования данных в векторы и обратно, операции с ними. Узкая направленность. Использовать MatLab можно только в его замкнутой экосистеме, на других программных платформах этот язык неэффективен. Высокая стоимость. Программная среда распространяется платно. Для покупки по минимальной стоимости нужно быть студентом образовательного учреждения. Также алгоритмы являются проприетарными, поэтому просмотр кода большей их части недоступен [4]	Цены варьируются в зависимости от выбранного вами варианта языка	Благодаря своему широкому использованию в различных количественных вычислениях как для научных целей, так и для целей индустрии, MATLAB стал достойным вариантом для применения в области науки о данных. Он придется вам как нельзя кстати, если для ваших ежедневных целей необходима интенсивная, продвинутая математическая функциональность, собственно, для чего MATLAB и был разработан.

Для проведения сравнительного анализа будет использоваться метод идеальной точки. Для проведения расчетов используем Excel MS, так как он доступен и удобен. Экспертами будут сотрудники ЦЦ и персонал со стороны подрядчика, занимающийся настройками интеграций. Оценку будем проводить по основным критериям:

- 1) функциональность – оценивание обширность функциональных возможностей языка, относительно всех вариантов;
- 2) доступность – оценивание сложность установки языка для текстовых редакторов;
- 3) производительность – оценивание результативности и эффективности языка в предметной области;

- 4) надежность – оценивание влияния команд языка программирования на данные;
- 5) направленность на предметную область;
- 6) поддержка разработчиков и сообщества.

Метод идеальной точки. Рассматривается m -мерное пространство (где m – число локальных критериев), в котором априори выбирается вектор, отображающий идеальное решение (или, что-то же самое, идеальная точка, координатами которой являются идеальные значения (например, минимальные или максимальные значения) локальных критериев). В этом пространстве вводится некоторая метрика, с целью вычисления расстояния между вектором, отображающим рассматриваемое решение, и идеальным. В качестве наилучшего выбирается такое решение, векторная оценка которого наиболее близка к идеальной точке.

Были выделены шесть критериев для сравнения, по которым эксперты выставили баллы оценки. Далее по каждому критерию находится наилучшее значение и заносится в столбец условного эталонного объекта. Затем необходимо посчитать стандартизированные показатели по формуле (1):

$$x_{ij} = \frac{a_{ij}}{\max a_{ij}}, \quad (1)$$

где x_{ij} – стандартизированные показатели, a_{ij} – исходные показатели.

В результате нужно определить рейтинговую оценку каждого редактора по формуле (2):

$$R_j = \sqrt{K_1(1 - X_{1j}^2)^2 + \dots + K_n(1 - X_{nj}^2)^2}, \quad (2)$$

где $K_1, K_2, \dots, K_n$ – весовые коэффициенты показателей, назначаемые экспертом.

В табл. 2 представлено сравнение языков программирования с помощью метода идеальной

Таблица 2

Сравнение языков программирования по методу идеальной точки

Показатели		Анализируемые языки программирования								Условный эталонный инструментарий	Весовые показатели
		Python		SQL		Java		Matlab			
		Баллы	Стандартизированные показатели	Баллы	Стандартизированные показатели	Баллы	Стандартизированные показатели	Баллы	Стандартизированные показатели		
1	Функциональность	9	0,90	7	0,70	8	0,80	10	1,00	10	0,20
2	Доступность	9	1,00	9	1,00	8	0,89	4	0,44	9	0,20
3	Производительность	9	0,90	8	0,80	10	1,00	9	0,90	10	0,10
4	Надежность	8	0,80	7	0,70	9	0,90	10	1,00	10	0,20
5	Направленность на предметную область	10	1,00	9	0,90	9	0,90	10	1,00	10	0,20
6	Поддержка разработчиков и сообщества	9	1,00	8	0,89	9	1,00	9	1,00	9	0,10
Рейтинговая оценка		0,19		0,36		0,22		0,36		Итого:	1
Рейтинговое место		1		3		2		4			

На основе проведенных расчетов составим для каждого языка программирования лепестковые диаграммы для наглядной демонстрации рейтинговой оценки (рис. 13).

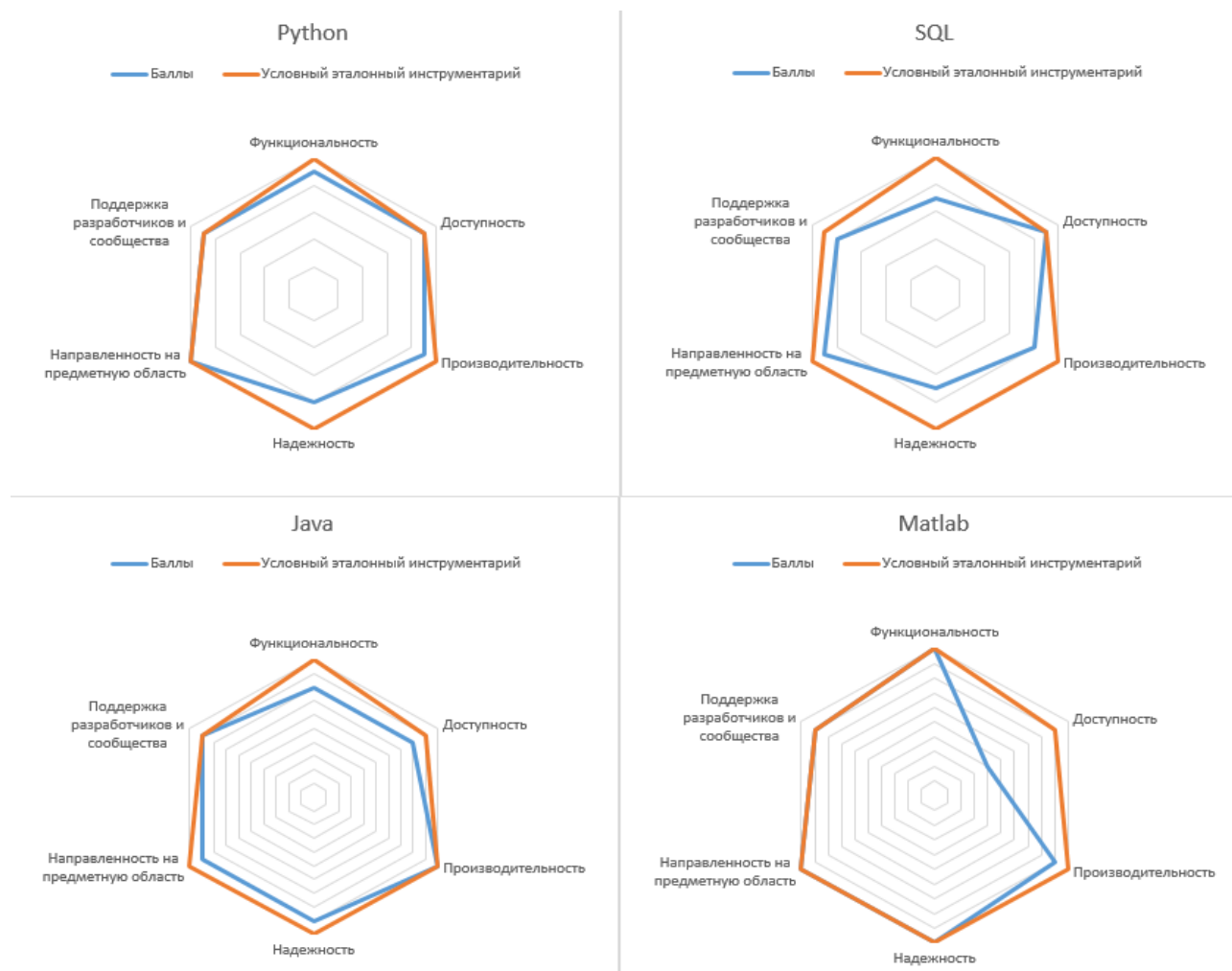


Рис. 13. Лепестковые диаграммы отклонение оценок вариантов от эталонных

На диаграммах отклонение у Python, наибольшее у SQL. На основе оценок было принято решение использовать для разработки инструмента Python, для контроля его точности SQL в БД Подсистемы.

Обоснование метода проектирования объекта исследования

Метод проектирования определяет работу по разработке инструмента и внедрению его в деятельность Ситуационного центра. При выборе метода стоит определить требования к инструменту и самому методу.

Ранее было определено, что инструмент должен быть разработан вручную, а также необходимо его корректировать снова и снова на протяжении пользования интегрировании данных в Подсистему.

Модели жизненного цикла информационных систем разделяют на каскадную, итерационную и спиральную. Из них под наш проект подойдет спиральная, так как подразумевает несколько версий одного продукта. На рис. 14 показана схема спиральной модели.

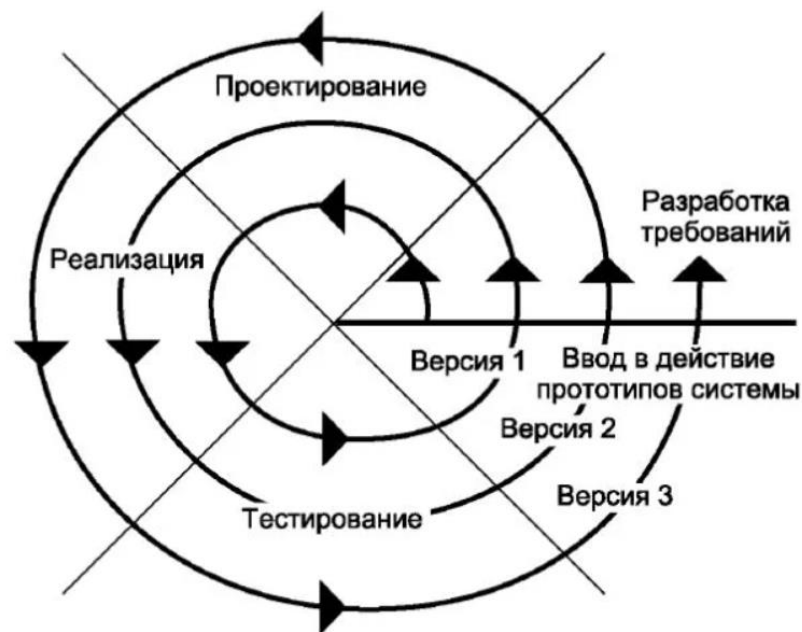


Рис. 14. Схема спиральной модели ЖК

Под такую модель подходят методы XP и RAD.

Технология XP связана со стремлением авторов (К. Бек, У. Каннингем, М. Фаулер) поднять существующие методы разработки ИС на новый уровень. Для оценки проектов применяются два показателя – критичность и масштаб. Критичность определяется последствиями, масштаб – количеством работников.

Технология RAD (англ. Rapid Application Development) основана на спиральной модели жизненного цикла и обеспечивает ускорение разработки ИС благодаря широкому привлечению к процессу проектирования будущих пользователей. Для данной технологии характерно перенесение основных работ с предпроектной стадии на проектирование.

Применение технологии RAD – наиболее подходящее для разработки инструмента по проверки работоспособности. Для проекта не так важны масштаб или количество разработчиков, поэтому технологию XP использовать не целесообразно.

В технологии RAD разделяют несколько видов прототипов: горизонтальный, вертикальный, одноразовый и эволюционный.

Для горизонтального важен интерфейс приложения и ему уделяется наибольшее внимание при разработке. В вертикальном прототипе важны все срезы приложения. Одноразовый применяется для решения проблемы единой, без дальнейшего пользования прототипом.

Эволюционный прототип подходит для проекта разработки, так как этот прототип подразумевает совершенствование продукта на следующих итерациях.

Для описания проектной деятельности необходимо определить методологию. Использовать будем методологию RUP, так как его используют при спиральной модели ЖК. В качестве языка моделирования используется Unified Modelling Language (UML).

Наибольшее внимание RUP уделяет начальным стадиям разработки проекта – анализу и моделированию – что призвано снизить риски проекта за счет раннего обнаружения возможных ошибок. Последовательный выпуск версий организован таким образом, чтобы наиболее существенные риски устранялись в первую очередь.

Итак, для разработки инструмента проверки целостности данных были определены:

- Модель ЖК: Спиральная;
- Технология: RAD;
- Методология: RUP;

Заключение. На момент написания статьи уже разработана основа для инструмента. С помощью сценария, написанного на Python, можно выгружать таблицы из БД Подсистемы. Далее необходимо изучить методы исследования данных и применить их на действующие интеграции. После определения методов будет доработан основной сценарий.

Список литературы

1. Методические рекомендации по созданию и вводу в эксплуатацию ситуационных центров, работающих по единому регламенту взаимодействия, утвержденные решением Межведомственной комиссии по координации деятельности федеральных органов исполнительной власти по созданию системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия (протокол № 2 от 7 мая 2015 г.)

2. 13 лучших инструментов для анализа данных, 11.07.2021 // New-science [Электронный ресурс]. – URL: <https://new-science.ru/13-luchshih-instrumentov-dlya-analiza-dannyh/?ysclid=lx097naokh203391547> (дата обращения: 01.09.2024).

3. Data Validation: Types, Benefits, and Accuracy Process, 21.12.2023 // Atlan [Электронный ресурс]. – URL: <https://atlan.com/what-is-data-validation> (дата обращения: 01.09.2024).

4. MatLab // Skillfactory media [Электронный ресурс]. – URL: <https://blog.skillfactory.ru/glossary/matlab> (дата обращения: 01.09.2024).

5. Mona Rakibe, Why Data Validation Matters: 8 Steps to Boost Data Quality & Value // Telmai [Электронный ресурс]. – URL: <https://www.telm.ai/blog/8-must-follow-steps-to-ensure-successful-data-validation> (дата обращения: 01.09.2024).

6. Sebastian Taylor, Data Validation // CFI [Электронный ресурс]. – URL: <https://corporatefinanceinstitute.com/resources/data-science/data-validation> (дата обращения: 01.09.2024).

7. Top 15 Automation Tools for Data Analytics, 10.01.2024 // Geeksforgeeks [Электронный ресурс]. – URL: <https://www.geeksforgeeks.org/top-15-automation-tools-for-data-analytics> (дата обращения: 01.09.2024).

8. What is data validation? // TIBCO [Электронный ресурс]. – URL: <https://www.tibco.com/glossary/what-is-data-validation#:~:text=Data%20validation%20is%20the%20process,validation%20to%20ensure%20accurate%20results> (дата обращения: 01.09.2024).

9. Громов В. SQL: что это и зачем // Курсы.ру [Электронный ресурс]. – URL: <https://kursy.ru/znaniya/programmirovaniye/chto-takoe-sql-i-zachem/> (дата обращения: 01.09.2024).
10. Дэвид Тейлор. 25 лучших бесплатных инструментов для интеллектуального анализа данных (2024 г.), 05.01.2024 // Guru [Электронный ресурс]. – URL: <https://www.guru99.com/ru/best-data-mining-tools.html> (дата обращения: 01.09.2024).
11. Единый регламент взаимодействия распределенных ситуационных центров, утвержденный решением Межведомственной комиссии по координации деятельности федеральных органов исполнительной власти по созданию системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия (протокол №2 от 07.05.2015).
12. Интеграция данных // Tadviser [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/Статья:Интеграция_данных (дата обращения: 01.09.2024).
13. Интеграция данных в компании: Что это? Как? И зачем? // DataReview [Электронный ресурс]. – URL: <https://datareview.info/article/integraciya-dannyx-v-kompanii-chto-eto-kak-i-zachem/> (дата обращения: 01.09.2024).
14. Интеграция информационных систем: виды и применение // Deco system [Электронный ресурс]. – URL: <https://www.decosystems.ru/typy-integratsii-informatsionnykh-sistem/?ysclid=1wyofgu26n497266366> (дата обращения: 01.09.2024).
15. Кому и для чего нужен Java? // Skillfactory media [Электронный ресурс]. – URL: <https://blog.skillfactory.ru/komu-i-dlya-chego-nuzhen-python/>
16. Кому и для чего нужен Python? // Skillfactory media [Электронный ресурс]. – URL: <https://blog.skillfactory.ru/komu-i-dlya-chego-nuzhen-python/> (дата обращения: 01.09.2024).
17. Малков А. В. Создание интегрированных систем менеджмента – один из механизмов реализации целей устойчивого развития // Менеджмент в России и за рубежом. – 2019. – № 3. – С. 36–40.
18. Анвар М. Рейтинг инструментов проверки данных, которые стоит изучить 2024. 20.03.2024 // Astera [Электронный ресурс]. – URL: <https://www.astera.com/ru/type/blog/data-validation-tools/> (дата обращения: 01.09.2024).
19. Методы исследований в менеджменте : учеб. пособие / А. Е. Плахин, Е. С. Огородникова, М. С. Хохолуш [и др.]. – Екатеринбург : Изд-во УрГЭУ, 2020. – 248 с.
20. Методы проверки данных: раскрытие бизнес потенциала: стратегии проверки данных для стартапов, 23.03.2024 // FasterCapital [Электронный ресурс]. – URL: <https://fastercapital.com/ru/content/Методы-проверки-данных--раскрытие-бизнес-потенциала--стратегии-проверки-данных-для-стартапов.html> (дата обращения: 01.09.2024).
21. Постановление Администрации Волгоградской области от 23 мая 2011 года № 244-п «Об организации межведомственного информационного взаимодействия в Волгоградской области».

22. Распоряжение комитета информационных технологий и коммуникаций Волгоградской области от 1 июня 2011 года № 03-о/д «О мерах по реализации постановления Администрации Волгоградской области от 23 мая 2011 года № 244-п «Об организации межведомственного информационного взаимодействия в Волгоградской области».

23. Тюфякова В. 9 языков программирования для работы с Big Data // Skillfactory media [Электронный ресурс]. – URL: <https://blog.skillfactory.ru/9-yazykov-dlya-raboty-s-big-data/> (дата обращения: 01.09.2024).

24. Управление качеством и интегрированные системы менеджмента : учебник / А. В. Аверин, Т. В. Барт, С. А. Бука [и др.] ; под ред. А. В. Аверина. – М.: КноРус, 2020. – 357 с.

25. Федюкин В. К. Управление качеством производственных процессов : учеб. пособие. – М.: КноРус, 2018. – 229 с.

26. Что такое интеграция данных? // SAP [Электронный ресурс]. – URL: <https://www.sap.com/central-asia-caucasus/products/technology-platform/what-is-enterprise-integration/data-integration.html> (дата обращения: 01.09.2024).

27. Шарафутдинова Е. Н. Системы инструментов управления качеством : учеб. пособие / Е. Н. Шарафутдинова, О. В. Плинка. – Екатеринбург: Издательство УрГЭУ, 2021. – 180 с.

Е. М. Дубовикова,

кандидат педагогических наук, доцент,
Волгоградский государственный университет
(Волжский филиал)

Г. Г. Егоров,

кандидат юридических наук, доцент,
Волгоградский государственный университет
(Волжский филиал)

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ НЕЙРОСЕТЕЙ ПРИ ИЗУЧЕНИИ АНГЛИЙСКОГО ЯЗЫКА

Аннотация. В данной статье рассматривается применение нейросетей в обучении иностранным языкам. Проанализировано, как задания и тексты, созданные нейросетями, могут быть использованы в учебном процессе. Кроме того, в статье уточняется понятие «искусственный интеллект» в контексте обучения языкам. Исследуется практическое применение искусственного интеллекта в образовании, особенно в обучении иностранным языкам. Утверждается, что программы искусственного интеллекта могут успешно персонализировать обучение, повысить мотивацию учащихся, существенно сократить время преподавателей на подготовку материалов и позволить им сосредоточиться на более творческих аспектах своей работы.

Ключевые слова: изучение английского языка, нейросети, машинный контроль, контроль освоения курса, современные технологии

USING MODERN NEURAL NETWORKS IN LEARNING ENGLISH

Abstract. This article discusses the use of neural networks in teaching foreign languages. The authors analyze how tasks and texts created by neural networks can be used in the educational process. In addition, the article clarifies the concept of "artificial intelligence" in the context of language teaching. The article explores the practical application of artificial intelligence in education, especially in teaching foreign languages. The authors argue that artificial intelligence programs can successfully personalize learning, increase student motivation, significantly reduce the time teachers spend preparing materials and allow them to focus on more creative aspects of their work.

Keywords: learning English, neural networks, machine control, course completion control, modern technologies

Введение. Современный педагог должен не только глубоко владеть предметом и методами преподавания, но и обладать знаниями о когнитивных процессах человека: как мозг воспринимает и обрабатывает информацию, как он реагирует на изучение новых языков. Помимо этого, педагог должен уметь строить эффективные межличностные отношения с учениками.

Современные педагоги часто совмещают преподавание с созданием собственных методик и курсов. Для этого необходимо глубокое понимание особенностей языкового обучения у детей и взрослых, а также механизмов перевода пассивного словаря в активный. Идея объединения педагогики и лингвистики активно развивалась в трудах отечественного психолога Л. С. Выготского. Сегодня одним из лидеров, как отмечают ряд авторов, в этой области является Татьяна Черниговская, благодаря которой нейролингвистика стала популярной в России [1].

Основная часть. Формирование навыков иностранного языка является ключевым показателем успешности обучения как в школе, так и в университете. Для эффективного развития лексических навыков у школьников необходимо сочетать классические методы обучения с современными информационными технологиями, включая мобильные приложения и нейронные сети.

Отдельно стоит рассмотреть понятие искусственного интеллекта, его уровень интеллектуальности и причины, по которым он называется «искусственным».

Данная тема крайне актуальна и требует всестороннего освещения. Проблематика, которую она поднимает, должна стать предметом пристального внимания лингвистов, методистов и преподавателей.

Используя нейросеть, можно автоматически создавать разнообразные образовательные материалы, такие как тесты. Нейросеть анализирует предоставленную информацию и генерирует задания разных типов (тесты, кроссворды, вопросы, интерактивные диаграммы и другие) в соответствии с тематикой и структурой материала [7].

Анализ последних исследований показывает, что студенты все чаще используют нейросети в вузовской учебе. Распространены случаи написания выпускных квалификационных работ и других заданий с помощью нейросетей,

включая перевод текстов с помощью онлайн-сервисов. В 2023 году Хайкин, Саймон выпустил издание, призывающая научное сообщество обсудить как преимущества, так и риски использования искусственного интеллекта в образовании [8].

Эксперты указывают на ряд недостатков систем искусственного интеллекта: ненадежность данных (система работает с текстами, созданными людьми, не учитывая контекста их создания) и генерацию ложной информации (даже последние версии чат-ботов могут создавать неверный контент) [8]. Тем не менее большинство экспертов в образовании считают, что полный запрет нейросетей нецелесообразен. Однако они предлагают обязательное указание на использование искусственного интеллекта в процессе работы.

Важно осознавать, что искусственный интеллект способен создавать текст на основе доступной в сети информации, но только человек может делать выводы, интерпретировать данные и формировать оригинальные суждения.

Безусловно, искусственный интеллект уже успешно применяется для обучения иностранным языкам. В 2023 году в российских научных изданиях было опубликовано множество исследований, посвященных различным аспектам использования нейронных сетей в языковом обучении. Например, рассматривались перспективы применения нейросетей в дебатах (Ю. В. Шуйская, Е. А. Дроздова, М. В. Мыльцева) [6], создание нейросетевых систем тестирования языковых компетенций (Е. М. Базанова, А. В. Горизонтова, Н. Н. Грибова и др.), использование нейросетей для языковой подготовки студентов технических вузов (М. Г. Евдокимова, Р. Т. Агамалиев) и повышение мотивации студентов к изучению иностранных языков (О. В. Мещеркова).

Подводя итог опыту применения нейросетей в образовании, нельзя не упомянуть об их использовании в онлайн-обучении. Существуют программы, способные подбирать учебные материалы индивидуально для каждого обучающегося в зависимости от его потребностей и уровня владения иностранным языком (например, Knewton, Learn-dash).

Многие образовательные платформы, представляющие собой персонализированные онлайн-ресурсы с учебными материалами, используют адаптивные технологии, позволяющие анализировать исходные данные пользователей и обрабатывать их для создания индивидуальных учебных планов [2].

Определив пробелы в знаниях учащихся, платформа фокусируется на их устранении [4]. Функционал таких систем с искусственным интеллектом обширен: они не только персонализируют обучение (предоставляют индивидуальные подсказки и траектории), но и помогают создателям курсов организовать мгновенную обратную связь, отслеживать прогресс, составлять расписания и многое другое.

Яркими примерами использования искусственного интеллекта в онлайн-обучении иностранным языкам являются образовательная платформа Duolingo и приложение Virtual Talk, позволяющие практиковаться в устной и письменной речи с помощью мультимедийных материалов. Далее рассмотрим, как преподаватель иностранного языка может использовать возможности искусственного интеллекта в процессе обучения.

Полагаем, что ключевое преимущество искусственного интеллекта в обучении иностранным языкам заключается в возможности персонализации обучения, что повышает мотивацию учащихся и сокращает время подготовки преподавателей. Благодаря персонализации создается комфортная учебная среда, формируется положительное отношение к изучению языка, что в итоге способствует более эффективному усвоению материала [9].

Считаем крайне важным вовлекать обучающихся в интерактивные истории, актуальные и лично значимые для них, чтобы поддерживать мотивацию к изучению языка. Нейросети позволяют создавать такие истории с разнообразными персонажами [3]. Например, если ученик не понял грамматическую тему или испытывает трудности с усвоением лексики, искусственный интеллект может генерировать специальные задания, адаптированные к его индивидуальным потребностям и учитывающие объем и сложность материала.

В учебники часто выносятся активная и пассивная лексика, которая затем встречается редко. Некоторые ученики быстро запоминают новые слова, видя их пару раз в контексте, в то время как другим требуется дополнительная практика. В таких случаях нейросети могут стать незаменимым инструментом, позволяя быстро создавать разнообразные упражнения для закрепления лексики, одновременно развивая навыки аудирования, чтения и письма.

На первом этапе с помощью нейросети, например, на сайте Artgeneration.me, можно создать изображение по заданным ключевым словам. Для закрепления лексики в восприятии речи можно сгенерировать сказку или рассказ на основе этих слов, используя нейросети и ресурсы вроде ChatGPT в Telegram или Perplexity.

Искусственный интеллект также может напоминать о необходимости повторения пройденного материала. Например, приложение Memrise позволяет определять объекты в реальном мире и получать их перевод. Допустим, направив камеру на стул, вы мгновенно узнаете, как это слово звучит на изучаемом языке [5].

Таким образом, можно заключить, что искусственный интеллект станет незаменимым помощником преподавателя в виртуальной реальности. Например, во время лекции, пока преподаватель объясняет материал, ИИ параллельно будет создавать визуальные материалы, такие как иллюстрации, инфографику или пояснения терминов, что сделает обучение более наглядным и эффективным.

Это не будут старые, устаревшие иллюстрации и примеры, которые используются уже двадцать лет. Искусственный интеллект будет создавать новые, актуальные материалы прямо во время урока и предоставлять их каждому ученику индивидуально. Ученики смогут самостоятельно взаимодействовать с этими материалами: увеличивать, поворачивать, удалять. Весь сгенерированный ИИ контент будет сохраняться для последующего просмотра.

Использование преподавателем нейросетей может значительно изменить его работу. Это открывает новые возможности для творческого подхода к подготовке занятий. Нейросети не заменят преподавателя полностью, но помогут учителям, которые умеют применять технологии искусственного интеллекта. Безусловно нейросети не смогут заменить преподавателя, однако как отмечает

И. М. Реморенко «...учителя заменит другой учитель, который умеет пользоваться технологиями искусственного интеллекта» [1].

Заключение. Если раньше работа с интернет-технологиями требовала особых навыков от преподавателя, то теперь мы приближаемся к будущему, где искусственный интеллект станет такой же неотъемлемой частью языковых курсов (онлайн и офлайн), как видео- или аудиоматериалы. Со временем больше программ по использованию искусственного интеллекта в образовании станут доступнее. Главное, что требуется от учителя, – это воображение и критическое мышление, чтобы оценивать и корректировать задания и тексты, созданные искусственным интеллектом, при необходимости.

Список литературы

1. Российская газета – Федеральный выпуск: № 13(9255) [Электронный ресурс]. – URL: https://rg.ru/2024/01/19/pravila-dlia-nejroseti-rektor-mgpuigor-remorenko-rasskazal-ob-iskusstvennom-intellekte-obrazovani.html?utm_campaign=news_january_2024_vypusk_2&utm_medium=email&utm_source=Sendsay (дата обращения: 01.09.2024).
2. Белоусова Л. И., Олефиренко Н. В. Дидактический потенциал цифровых образовательных ресурсов для младших школьников // ОТО. 2013 № 1. [Электронный ресурс]. – URL: <https://cyberleninka.ru/article/n/didakticheskiy-potentsialtsifrovyyh-obrazovatelnyh-resursov-dlya-mladshih-shkolnikov> (дата обращения: 01.09.2024).
3. Дахин А. Н., Семенов Н. Г., Ярославцева Н. В., Ермолаев С. Ю. Педагогические технологии и нейросети // Школьные технологии [Электронный ресурс]. – 2020. – № 2. – С. 28–33.
4. Дубовикова Е. Ю., Егоров Г. Г. Современные тенденции развития высшего образования в цифровой экономике // Энергетика в условиях цифровой трансформации. Наука. Технологии. Инновации: сборник материалов Международной научно-практической конференции. – Волжский, 2022. – С. 252–256.
5. Искусственный интеллект в изучении иностранных языков [Электронный ресурс]. – URL: <https://mel.fm/blog/maksim-sundalov/65742-iskusstvenny-intellekt-v-izuchenii-inostrannykh-yazykov> (дата обращения: 01.09.2024).
6. Нейросеть генерирует упражнения для изучения языков по фотография [Электронный ресурс]. – URL: <https://neurohive.io/ru/gotovye-prilozheniya/nejroset-generiruet-uprazhneniya-dlya-izucheniya-yazykov-po-fotografiyam> (дата обращения: 01.09.2024).
7. Рассел С., Норвиг П. Искусственный интеллект. Современный подход. – БХВ-Петербург, 2013. – 480 с.
8. Хайкин С. Нейронные сети. Полный курс. – М.: Издательский дом «Вильямс», 2006. – 486 с.
9. Krasilnikova T. K., Egorov G. G., Ryabova E. V., Dubovikova E. Y. The influence of information and computer technologies and transnational media corporations on public legal awareness // Digital Future Economic Growth, Social Adaptation, and Technological Perspectives. Switzerland, 2020. – С. 645–652.

О. В. Киселкина,

кандидат экономических наук, доцент,
Казанский (Приволжский) федеральный университет

РАЗВИТИЕ ЦИФРОВИЗАЦИИ РЕКРУТМЕНТА

Аннотация. Рекрутмент постоянно трансформируется с развитием цифровых технологий. Цифровые технологии в отборе персонала позволяют создать новые модели и совершенствовать HRM-системы. В статье проведен анализ развития автоматизации рекрутмента, функционал цифровых инструментов, возможности и вызовы использования искусственного интеллекта в сорсинге, систем автоматизации рекрутинга, проведена оценка их эффективности.

Ключевые слова: цифровые технологии, рекрутинг, HR-процессы, сорсинг, автоматизация процессов, искусственный интеллект

DEVELOPMENT OF DIGITALIZATION OF RECRUITMENT

Abstract. The process of recruitment is constantly transforming with the development of digital technologies. Digital technologies in personnel selection allow creating new models and improving HRM systems. The article analyzes the development of automation in recruitment, the functionality of digital tools, the possibilities and challenges of using artificial intelligence in sourcing, and recruitment automation systems, and assesses their effectiveness.

Keywords: digital technologies, recruitment, HR processes, sourcing, automation of processes, artificial intelligence

Введение. Подбор и отбор персонала относится к главным процессам, от которых зависит конкурентоспособность и эффективность деятельности любой организации. Применение цифровых инструментов в этих процессах стало необходимостью по многим причинам. Цифровые инструменты позволяют сокращать временные затраты на сбор и обработку данных, оптимизировать трудовые, материальные и финансовые ресурсы, а также повышать их качество.

Основная часть. Приоритетным направлением для большинства организаций стала автоматизация многих функций управления персоналом, прежде всего кадрового делопроизводства, расчета вознаграждения и льгот, обучения и развития, рекрутмент и оценка персонала [4]. Как правило, автоматизируются процессы с наибольшим количеством вариаций сценариев выполнения, подразумевающие действия с четкими инструкциями по обработке информации, основанные на шаблонах. Такие процессы подразумевают работу в Excel, Word, почтовыми сервисами и документами [3]. Помимо возможности автоматизации операционных и повторяющихся рутинных процессов рекрутеры активизируют применение роботизации и искусственного интеллекта в осуществлении своей деятельности. Анализ данных и их глубокое изучение позволяет руководителям и рекрутерам получить полноценную картину процесса отбора персонала, выявить основные проблемы и погрешности в процессе и усовершенствовать процесс рекрутинга в соответствии с полученными данными [2].

Цифровые инструменты в отборе персонала на начальном этапе помогают отфильтровать кандидатов на вакантные должности по заранее заданным параметрам. Крупные компании проводят скрининг резюме, особенно при массовом подборе. Автоматизация больших объемов резюме позволяет намного повысить эффективность работы рекрутера. Программа удаляет резюме, не прошедшие первичный отбор, и рекрутер в дальнейшем оценивает компетенции соискателя по критериям, не учтенным при первичном отборе.

Поиск кандидатов не ограничивается сбором откликов на вакансию. В условиях кадрового дефицита рекрутер ищет подходящих людей на позицию с помощью сорсинга. Правильно сформулированные параметры в заявке вакансии позволяют получить больше хороших откликов. При этом они должны учитывать как потребности в найме, так и желания кандидатов, а именно их ожидания от будущей работы, критерии поиска и выбора соответствующей вакансии. В первую очередь в заявке на подбор необходимо указывать условия работы с учетом реалий рынка труда и описание самой вакансии, во вторую – бренд работодателя. Каналами поиска кандидатов могут быть разные источники и площадки: Яндекс и Google, рабочие сайты, социальные сети, мессенджеры, профессиональные сообщества и пр. Современными инструментами в поиске становятся булевые запросы, x-гау поиск, сервисы и плагины для браузеров.

Для анализа и улучшения привлекательности объявлений о вакансиях компании используют искусственный интеллект (ИИ). Исследование Работа.ру выявило, что создают описание вакансий с помощью ИИ 14% респондентов, автоматизируют сортировку и отбор резюме – 5% [5]. Исследование, проведенное компанией «Поток» показало, что 12 процентов респондентов используют ИИ для автоматического подбора резюме [1].

Среди причин, по которым поиск с помощью искусственного интеллекта становится важным для рекрутеров, можно выделить следующие. Во-первых, конкуренция в рекрутинге усиливается. Спрос на квалифицированных и талантливых работников превышает предложение, поэтому рекрутерам необходимо найти более умные и эффективные способы поиска кандидатов. Методы подбора, которые работали раньше, снижают свою эффективность. Кандидаты по-разному реагируют на охват. Ожидания в отношении опыта кандидатов, скорости и предложения работы очень высокие.

Во-вторых, рост социальных сетей облегчил кандидатам поиск открытых вакансий и подачу заявок. Это способствовало увеличению числа неквалифицированных кандидатов, претендующих на вакансию, объем данных о вакансиях существенно вырос, объявления о вакансиях стали менее эффективными. Для поиска лучших кандидатов рекрутерам необходимо осуществлять поиск из большего числа источников и площадок. Поиск с помощью искусственного интеллекта предлагает данные о потенциальных кандидатах и помогает рекрутерам проводить более целенаправленный поиск, находить пассивных кандидатов, которые могут оказаться лучшими кандидатами на вакансию.

В-третьих, рост разнообразия форм занятости, в частности удаленного и гибридного формата работы, увеличил объем данных о вакансиях и претендентах. Анализ данных стал еще важнее для сужения списка кандидатов и создания шортлиста (короткого списка) для дальнейшей оценки кандидатов. С помощью

искусственного интеллекта предварительный отбор может быть выполнен быстрее и эффективнее, рекрутер будет детально изучать меньший список кандидатов, тем самым будет достигнута экономия времени служб управления персоналом.

Применение нейросетей в рекрутинге открывает новые возможности, но также имеет ограничения и порождает ряд вызовов. В сорсинге искусственный интеллект нельзя рассматривать как единую концепцию, его всегда следует переводить на язык конечного пользователя – рекрутера, то есть необходим баланс между цифровыми инновациями и человеческим взаимодействием. Большинство алгоритмов основывают свой интеллект на большой базе профилей. Каждый профиль имеет базовые точки данных, например, должность, местоположение, ключевые слова. Инструменты поиска ИИ интерпретируют эти данные и оценивают каждую базовую точку данных, затем ранжируют профили по наивысшему общему баллу.

Риски использования нейросетей возрастают, если алгоритмы обучены на недостаточном и несбалансированном наборе данных. Существует также проблема конфиденциальности и защиты данных в процессах найма

При работе с большим количеством данных становится все более важным правильно управлять этими данными. Анализ данных применяется при глубоком изучении рынка труда, по результатам которого составляется карта поиска талантов, что в дальнейшем помогает быстро и качественно закрывать вакансии. Все большее внимание привлекает аналитика по этапам подбора, которая показывает, сколько кандидатов на каждом этапе отбора и как улучшить конверсию в найм. Управление эффективностью процесса подбора персонала заключается в оптимальном управлении бюджетом через рациональное использование сервисов.

Инструментом, который управляет профилем кандидатов, базами данных профилей и точками соприкосновения на протяжении всего процесса подбора персонала, являются система автоматизации рекрутмента – ATS (система отслеживания кандидатов). Такая система выполняет функцию централизованной информационной базы и помогает публиковать вакансии на рабочих сайтах и социальных сетях, хранить информацию о кандидатах (как активных, так и пассивных), собирать фидбэк по кандидатам, отправлять кандидатам первичные сообщения, собирать отклики и ответы кандидатов.

ATS имеют облачный вид и обеспечивают рекрутерам удаленный доступ к системе, в том числе через мобильные устройства. Такие системы имеют встроенную прикладную аналитику, что ускоряет анализ данных по метрикам процесса отбора персонала и позволяет влиять на показатели и результаты. К примеру, с помощью аналитики можно найти слабые места в вакансиях и понять, в какой мере они соответствуют рынку и что препятствует найму лучших кандидатов. В то же время можно отследить работу рекрутеров, сравнить их по эффективности работы, равномерности распределения нагрузки и оптимизировать численность сотрудников. Добавление в ATS компонента ИИ делает этот инструмент более интеллектуальным. ATS автоматически формирует разные типы отчетов, сокращая затраты времени рекрутера и уменьшая вероятность ошибки.

Сложность реализации функций подбора и отбора в управлении персоналом заключается в том, что специалисту по управлению персоналом или рекру-

теру важно понимать все детали вакантной должности и подобрать кандидата с учетом разных характеристик, а для этого ему необходимо обладать не только компетенциями менеджера и психолога, но и уметь работать с данными с применением цифровых технологий.

Заключение. Таким образом, процесс подбора и отбора персонала будет непрерывно трансформироваться. Этим процессам важно оставаться гибкими к изменениям, поэтому рекрутеры постоянно стараются находить эффективные способы поиска квалифицированных кандидатов, обеспечивать упорядоченность данных и автоматизировать этапы отбора. Растущей тенденцией в рекрутинге является поиск с помощью искусственного интеллекта, инструменты которого помогают принимать решения на основе данных и сократить рутинные операции в рекрутменте.

Список литературы

1. ИИ становится помощником кадровых служб [Электронный ресурс]. – URL: <https://cio.osp.ru/news/020424-II-stanovitsya-pomoschnikom-kadrovyyh-sluzhb> (дата обращения: 07.08.2024).
2. Киселкина О. В. Инновационные подходы к процессам подбора и отбора персонала в организациях // Региональный экономический журнал. – 2022. – № 1(32). – С. 64–70.
3. Корпоративная стратегия цифровизации – подходы и технологии [Электронный ресурс]. – URL: http://www.fa.ru/org/chair/bi/Documents/TK_Digital_Strategy.pdf. (дата обращения 02.09.2024).
4. Развитие HR-процессов и использование digital-инструментов в российских компаниях. / HeadHunter [Электронный ресурс]. – URL: <https://hhcdn.ru/file/16480569.pdf> (дата обращения: 12.09.2024).
5. Российские компании рассказали, как используют ИИ в работе [Электронный ресурс]. – URL: <https://press.rabota.ru/rossiyskie-kompanii-rasskazali-kak-ispolzuyut-ii-v-rabote> (дата обращения: 20.08.2024).

О. В. Кочеткова,

доктор технических наук, профессор

С. В. Вольф,

магистрант,

Волгоградский государственный аграрный университет

Е. А. Беликова,

кандидат медицинских наук, доцент,

Волгоградский государственный медицинский университет

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ЭФФЕКТИВНОГО ЛЕЧЕНИЯ ПАЦИЕНТОВ С ХРОНИЧЕСКИМ ГЕПАТИТОМ С

Аннотация. Работа посвящена актуальной теме повышения эффективности лечения воспалительного заболевания печени, вызываемого вирусом гепатита С (ХГС). Выполняется разработка интеллектуальной советующей системы

с целью уменьшения ошибок и повышения обоснованности принимаемых решений при выборе методов лечения больных ХГС.

Ключевые слова: интеллектуальные советующие системы, хронический вирусный гепатит С, эффективность лечения

ARTIFICIAL INTELLIGENCE TECHNOLOGY FOR EFFECTIVE TREATMENT OF PATIENTS WITH CHRONIC HEPATITIS C

Abstract. The work is devoted to the current topic of increasing the effectiveness of treatment of inflammatory liver disease caused by the hepatitis C virus (CHC). The authors of the study are developing an intelligent advisory system in order to reduce errors and increase the validity of decisions made when choosing treatment methods for patients with CHC.

Keywords: intelligent advisory systems, chronic viral hepatitis C, treatment effectiveness

Введение. Современные информационные технологии играют ключевую роль в развитии различных отраслей, они в последнее время все шире используются в медицине. Одним из перспективных направлений является применение интеллектуальных систем для поддержки принятия решений, что особенно важно для медицинской отрасли.

Основная часть. Вирус гепатита С (ВГС) является одним из наиболее частых этиологических агентов, которые способствуют возникновению хронических заболеваний печени. Несмотря на довольно высокую заболеваемость хроническим вирусным гепатитом С (CHCV) в нашей стране (более 5 миллионов человек) наблюдается тенденция роста заболеваемости.

Министерство здравоохранения РФ отмечает серьезные проблемы, связанные с данной инфекцией, так как вирусный гепатит представляет угрозу общественному здравоохранению наравне с вирусом иммунодефицита человека (ВИЧ), малярией и туберкулезом. У гепатита С высокая частота формирования хронических форм, длительное бессимптомное течение, манифестация заболевания на поздних стадиях цирроза печени, четкая ассоциация с развитием гепатоцеллюлярной карциномы [4, 5].

На сегодняшний день уже накопленный богатый опыт ведения и лечения пациентов с гепатитом С, а также быстрое развитие высокоэффективной противовирусной терапии инфекции HCV обусловили потребность в современном инструменте для медицинских работников по выбору эффективных схем лечения пациентов с CHCV. Однако требуется глубокий системный анализ совокупности факторов, влияющих на выбор наилучших и результативных методик лечения этого заболевания.

Установлено [5], что на выбор тактики лечения больных с хроническим гепатитом С оказывают влияние следующие факторы:

- стадия фиброза печени, наличие цирроза печени и его класс;
- генотип вирусного гепатита С;
- наличие некоторых сопутствующих заболеваний;
- беременность;
- опыт предыдущей противовирусной терапии (если есть);

– прием лекарственных средств по поводу сопутствующей патологии.

Большая генетическая неоднородность вируса гепатита С проявляется в различных механизмах заражения и проявления, тяжести лечения, а также в особенностях диагностики, что обуславливает высокую сложность определения рациональных и эффективных схем лечения.

Разработка советующей системы соответствует методам интеллектуальной экспертных систем, так как решаемая задача обладает совокупностью нескольких определяющих характеристик [5]:

- задача имеет эвристическую природу, может быть решена естественным образом с помощью символических рассуждений;
- сложность задачи является приемлемой для использования методов искусственно интеллекта и, в то же время, задача достаточно сложна, что оправдывает затраты на разработку советующей системы;
- задача является достаточно узконаправленной и практически значимой.

Кроме того, успешность разработки и применения советующей системы в области лечения больных хроническим вирусным гепатитом С определяется тем, что существуют эксперты в данной предметной области, и они сходятся в оценке предлагаемых решений. Важно, что знания экспертов легко внести в советующую систему, так как эксперты способны объяснить используемые ими методы. Особенно необходимо отметить, что задача не является слишком трудной и ее решение требует не действий, а только рассуждений и не использует абстрактное мышление.

Проектирование и реализация интеллектуальной советующей системы, как и экспертных систем, реализуется на протяжении шести этапов: идентификация, концептуализация, формализация, реализация, тестирование и опытная эксплуатация.

В процессе идентификации были определены эксперты, знания которых будут заложены в систему, и официальные Клинические рекомендации Российского общества по изучению печени и Российской гастроэнтерологической ассоциации по диагностике и лечению фиброза и цирроза печени и их осложнений [3]. Кроме того, были определены типы пользователей советующей системы.

На этапе концептуализации был выполнен глубокий содержательный анализ предметной области и определено основное ограничение советующей системы: рассматривается лечение больного хроническим гепатитом С только одного типа и не болеющего ВИЧ инфекцией.

Заключение. В настоящее время выполняется реализация советующей системы путем разработки ее первого прототипа. Тестирование прототипа советующей системы предполагается провести на кафедре инфекционных болезней Волгоградского государственного медицинского университета силами клинических ординаторов и преподавателей. В случае наличия замечаний и ошибок в логических правилах базы знаний будет разработана вторая версия прототипа советующей системы, которая также будет протестирована.

Созданная советующая система уменьшит время, затраченное на выбор эффективных схем лечения больных с хроническим гепатитом С, снизит число ошибок в выборе эффективных схем лечения пациентов с хроническим гепатитом С.

Список литературы

1. Беликова Е. А. Эпидемиологические особенности гепатита С в Волгограде // Актуальные проблемы экспериментальной и клинической медицины: материалы 66-й открытой науч.-практ. конф. молодых ученых и студентов с междунар. участием. – Волгоград: ВолгГМУ, 2018. С. 132–133.
2. Беликова Е. А., Иоанниди Е. А., Попов С. Ф. Применение лайфферона в лечении больных хроническим гепатитом С (ХГС) // Российский журнал гастроэнтерологии, гепатологии и колопроктологии. – 2018. – № 1. – С. 29.
3. Ивашкин В. Т., Маевская М. В., Жаркова М. С., Жигалова С. Б., Киценко Е. А., Манукьян Г. В. (и др.) Клинические рекомендации Российского общества по изучению печени и Российской гастроэнтерологической ассоциации по диагностике и лечению фиброза и цирроза печени и их осложнений // Российский журнал гастроэнтерологии, гепатологии, колопроктологии. – 2021. № 31(6). С. 56–102.
4. Вольф С.В. Разработка концепции создания советующей системы по выбору эффективных схем лечения пациентов с хроническим гепатитом С//XVIII Международная научно-практическая конференция молодых исследователей «Наука и молодежь: новые идеи и решения», посвященная 80-летию со дня образования вуза, 20–22 марта 2024 г. – Волгоград: ВолГАУ, 2024. – С.124–128.
5. Клинические рекомендации «Хронический вирусный гепатит С» (утверждены Министерством здравоохранения РФ 29 декабря 2021 г. [Электронный ресурс]. – URL: https://hiv.sakhalin.gov.ru/site_get_file/1360/Klin%20rek%20HVG%20C.pdf
6. Экспертные системы [Электронный ресурс] // tadviser.ru – URL: https://www.tadviser.ru/index.php/Статья:Экспертные_системы_%28Разработка%29#.D0.A2.D1.80.D0.B5.D0.B1.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D1.8F.D0.BF.D0.BE.D1.81.D0.BE.D0.B7.D0.B4.D0.B0.D0.BD.D0.B8.D1.8E

Л. В. Кружалова,

кандидат исторических наук, доцент
Российский государственный педагогический
университет имени Герцена

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ХУДОЖЕСТВЕННОЙ ЛИТЕРАТУРЫ И ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРЕПОДАВАНИИ КОНФЛИКТОЛОГИИ

Аннотация. В статье рассматриваются практические примеры использования художественной литературы, документальных, художественных фильмов и мультфильмов для лучшего погружения в изучение предметов конфликтологического цикла.

Ключевые слова: коммуникация, конфликтология, бакалавры, студенты, учебники, литература, документальное, игровое кино

USING THE POSSIBILITIES OF FICTION AND DIGITAL TECHNOLOGIES IN TEACHING CONFLICT STUDIES

Abstract. The article discusses practical examples of the use of fiction, documentaries, feature films and cartoons for better immersion in the study of subjects of the conflict cycle.

Keywords: communication, conflictology, bachelors, students, textbooks, literature, documentary, feature films

Введение. Коммуникация в преподавании затруднена невероятной разностью культурного и словарного багажа поколений, как преподнести информацию, чтобы тебя поняли – крайне непростой вопрос. Необходимо искать и находить какую-то общую платформу, и здесь визуализация, цифровые технологии, наглядность будут незаменимы. Аристотелевские категории (действие, претерпевание, пребывание и обладание) работают также эффективно, как и во времена перипатетиков. Пятый элемент – память – включается на этой основе и позволяет оперировать полученной информацией уже осознанно. Задача преподавателя – заинтересовать, вовлечь в процесс исследования и закрепить полученные знания, которые должны быть выработаны самостоятельно, на базе критического мышления. Тогда результат обучения не выветрится из сознания студента после сдачи экзамена.

Основная часть. Дисциплина «конфликтология», которая преподается в разных ее модулях (история конфликтологии, введение в конфликтологию, общая конфликтология, юридическая конфликтология, технологии, институты конфликторазрешения и т. п.) представляет собой в любом варианте междисциплинарную, сложносоставную дисциплину, объединяющую социологию, философию, политологию, историю, психологию и некоторые другие дисциплины. Такая многозначность объясняется возрастающей ролью антропологии в гуманитарных науках, и тем, что в основании конфликтологии лежит диалектическое понимание конфликта. Эмпирическим материалом конфликтологии выступают различные сферы социальной практики: политика, образование и воспитание, наука, бизнес, производство, семья [3]. Изучение любого модуля основано на самостоятельном прочтении студентами значительного количества первоисточников – от Гомера до Лакана. С чтением книг, особенно с функциональным чтением уже давно существуют серьезные проблемы: студенты читают, конечно, но не ту литературу, которую необходимо, особенно проблематичным является знание (чтение) классической литературы. Она существует параллельно с существованием самих студентов: она сама по себе, они сами по себе, даже пересказ источников во Википедии осваивают единицы, и с каждым годом число и этих единиц уменьшается. Результатом является непонимание лекционного материала, формальный подход к практическим занятиям, крайне скудные знания профильных предметов, которые выявляются на государственных экзаменах и при защите ВКР. Основной компетенцией, которую массово осваивают студенты, является умение скопировать необходимую информацию из Интернета и выдать ее за свою при написании рефератов, курсовых, письменных ответов на практических занятиях. Книжная цивилизация медленно умирает, но смириться с этим невоз-

можно, поэтому в процессе изложения основных программных требований рабочих дисциплин по различным модулям необходимо использование литературных произведений – как отечественной, так и мировой классики. Отсылка к Гомеру, Шекспиру, Данте, Пушкину и другим гениям литературы отнюдь не означает, что студенты начнут их читать, но некоторые из них читают, и вот ради этих немногих имеет смысл не ограничиваться сухой терминологией учебника, а привлекать на помощь в изучении предмета труды литературных гениев, исправляя при этом первородный грех любого учебника: он скучен, написан, как правило, «деревянным» языком и не содержит ярких и запоминающихся примеров. Вот два примера из рекомендуемого учебника:

«Со временем менялись условия жизни, видоизменялись и конфликты. Иными становились их физические, экономические и социальные последствия. Не оставалось неизменным и отношение к ним общественной мысли. ... В Средние века и в Новое время были предприняты попытки осмыслить сущность этого явления. Целая плеяда мыслителей-гуманистов высказывала свои представления о конфликтах, пагубности их роли в развитии человечества, об устранении войны из жизни общества и установлении вечного мира» [1] (и на этом все – Прим. автора).

Или такое:

«Для усиления влияния конфликтологии на реальное поведение людей в проблемных ситуациях социального взаимодействия важно исследовать содержание накопленных в течение тысячелетий практических конфликтологических знаний. Такое исследование заметно расширит и углубит понимание конфликтов учеными. Вторая самостоятельная проблема – поиск путей коррекции обыденных конфликтологических знаний, приведение их в соответствие с научными знаниями о конфликтах» [1]. Для вчерашних школьников, «натасканных» на ЕГЭ, каждое слово нуждается в пояснении и примере, они ни понять, ни объяснить, ни пересказать даже такое не могут. Поэтому необходимо использовать имеющийся в арсенале преподавателя громадный, невостребованный научно-практический потенциал художественной литературы.

Именно художественная литература, в любом ее формате от сказки по эпосу помогает человеку понять и самого себя, и окружающих, и происходящие в мире и стране процессы. Гениальность хороших книг в том и состоит, что они существуют вне времени (война и предательство, измена и любовь, героизм и предательство) как причины конфликтов, как разные человеческие ценности, приводящие к конфликтам – одинаковы. Главная книга человечества – Илиада Гомера, история о Трое или Илионе, спетая Гомером. Этот эпос о нас самих, сегодняшних, как неразумно мы можем поступать, как можем перекидывать ответственность за то, что делаем, на других, на какое коварство и героизм мы, люди, способны. Эта книга отражает «что произошло тогда, что происходит сейчас и что будет происходить с человечеством до конца его существования» [2].

Изучение истории конфликтологии начинается именно с античной Греции, именно с Гомера: как люди понимали самого человека, как они представляли собственно человеческую природу, и какое влияние оказывали на него боги. Через тысячелетия пройдет тот же самый нарратив – что такое человек, в чем причины его конфликтности, может ли он властвовать собой, какова его свобода во-

ли, и, разбирая позже тему цели и средства в конфликте не обойтись без Раскольникова из «Преступления и наказания» Достоевского, без князя Андрея в «Войне и мире» Толстого, без Евгения в «Медном всаднике» Пушкина.

Центральная тема Средневековья – теоцентризм, ответственность за грехи человеческие, ответственность самого человека за свои действия очень сложно объяснить без Божественной комедии Данте. Кризис средневековой культуры, переход к антропоцентризму, человеку как творцу и центру Вселенной замечательно иллюстрирует Фауст, сочинение Гете. Если все Средневековье сверяло свою жизнь с Ветхим и Новым заветами, т. е. договорами с Богом, то Возрождение поставило вопрос об изменении этого договора. Для Фауста общение с дьяволом является жизненно необходимым, и исследование этого образа можно использовать при изучении раздела «Психологический подход в изучении конфликтологии». Фауст – это пример архетипа общеевропейского коллективного бессознательного, которое изучается и в творчестве Юнга, и в причинах внутриличностного конфликта: внутриличностный оппонент, темная сторона каждого человека, мрачные, темные качества человеческой натуры.

Война как силовой вариант подавления конфликтов может быть более понятна студентам, если в качестве дополнительного источника к теоретическим построениям использовать «Войну и мир» Л. Толстого и его же «Хаджи Мурата» «Кавказского пленника», «Казаков». Практически любая тема курса «история конфликтологии» опирается на тот или иной литературный шедевр. При разборе понятий «предмет конфликта», «вид конфликта», «участники конфликта» незаменимыми являются сказки А. С. Пушкина. На примере «Сказки о рыбаке и рыбке», «Сказки о золотом петушке», «Сказки о царе Салтане» студенты довольно быстро и безошибочно устанавливают предметы конфликтов, тем более что эти сказки им знакомы. Любой учебник дает такое определение:

«Предмет конфликта – это объективно существующая или воображаемая проблема, лежащая в основе конфликта (то, из-за чего возникает конфликт). Предметом может быть: конкретный объект (некий материальный предмет – один на несколько желающих); некая возможность (одна должность, на которую имеется более одного претендента); некое оценочное утверждение, оспариваемое другими; соблюдение/несоблюдение каких-то правил и т. п.»

Без пояснительных примеров понять, что такое предмет, вычленив его из сложной житейской ситуации невозможно и детские сказки приходят на помощь. В качестве более сложных заданий можно применять басни И. А. Крылова, в которых вычленив предмет бывает более трудно, но в качестве закрепления пройденного материала они вполне могут быть использованы. Литература – и отечественная, и зарубежная классика – есть яркая репрезентация конфликтологических идей. Как и другие виды искусства, литература представляет собой загадку человеческой иррациональности: «можно сказать, что литература предлагает описание конфликтологической реальности с различными вариантами стратегий поведения в ней субъектов» [3].

И Гомера, и Данте, и Гете и другую классику читают единицы из сотен студентов, но хотя бы в кратком пересказе, в минимальном знании для сдачи зачета/экзамена большинство получает общее представление.

На практических занятиях по конфликтологии должны использоваться примеры социальной жизни как в историческом, так и в культурно-антропологическом аспекте и в искусстве- картины, кинофильмы, примеры из сериалов, и т.п. должны сопровождать лекционный материал и использоваться на практических занятиях в качестве основного предмета изучения. Классическим примером комплексного иллюстративного применения классического произведения является «Мастер и Маргарита» М. Булгакова. Текст этого произведения знаком всем. Функциональное прочтение – практически никому, т. е. никакой контекст произведения не затрагивает юные умы: и кто такой чернокнижник Герберт Аврилакский, и какие доказательства бытия божия разрушил Кант, и какое новое доказательство он соорудил, и почему у Воланда болит колено, а Маргарите нужно целовать колено, и почему у Берлиоза и бездомного именно такие фамилии, и все-все остальное, крайне важное для понимания смысла романа не прочитывается, только фабула, только сюжет, но используя знание сюжета можно заинтересовать студентов, акцентируя их внимание на связь изучаемых тем со знакомыми эпизодами. Так, с Фомой Аквинским и Иммануилом Кантом мы знакомимся по известному монологу Воланда, с диалектикой Гегеля, в частности, по биографии Ивана Бездомного, ставшего Иваном Поныревым: как из глуповатого и нагловатого парня он превращается в уважаемого профессора, занимающегося очень неконъюнктурной темой – историей древней Иудеи. Этот роман, с которым знакомы все студенты, настоящий кладезь социологических, психологических, исторических, теологических примеров иллюстраций к курсу истории конфликтологии. Прекрасной возможностью проиллюстрировать сюжет являются сериалы 2005 и 2024 гг. В. Бортко и М. Локшина, нарезка кусочков сюжета используется как в дисциплине общая конфликтология, так и институтах конфликто-разрешения. Незаменим фильмы М. Голдовской «Власть Соловецкая» и М. Ромма «Обыкновенный фашизм». Дм. Лихачев, один из героев фильма М. Голдовской рассказывает о пережитом на камеру, очень редкие документальные кадры сопровождают рассказ, в просмотровом зале стоит мертвая тишина, и нет ни одного желающего достать мобильник. Для выполнения творческого задания на тему «Моя жизнь в Третьем рейхе» (опыт вымышленной биографии) студенты смотрят фильмы Л. Риффеншталь «Триумф воли» и «Олимпию», «Обыкновенный фашизм» М. Ромма (дисциплина Института конфликто-разрешения, опыт строительства тоталитарного государства). Для современных студентов визуальный ряд гораздо понятнее вербального. Если в одной из первых тем курса «введение в конфликтологию» показать несколько эпизодов из фильма Д. Сифроно «Дикие истории», то понимание того, что такое предмет конфликта, эскалация конфликта, и другие структурные элементы конфликта они не забывают никогда. Говорим о толерантности, смотрим мультимедиа «Голубой щенок», или «Гадкий утенок», обсуждаем проблемы непонимания- пожалуйста, есть «Медвежуть» и т. д.

По каждой сложной для понимания теме для студентов подобран определенный видеоряд, что не только разнообразит, собственно, саму лекцию, но, используя эмоциональный компонент, создает эффект присутствия. Почти как у Аристотеля.

К старшему, выпускному, четвертому курсу студенты вполне самостоятельно подбирают для практических занятий нарезки из мультфильмов (на первом месте тут «Смешарики»), выступлений стендаперов и т.п.

Изучение дисциплины правоведение представляет определенную сложность ввиду фрагментарного изучения основ правоведения в школе, при этом учебники по обществознанию также далеки от увлекательности, и очень многое зависит от учителя, преподающего данную дисциплину. Проводя предварительную проверку остаточных знаний по этому предмету перед началом занятий убеждаюсь, что таких практически нет, во всяком случае у подавляющего большинства первокурсников. Наиболее яркие и понятные примеры в мультфильмах «Трое из Простоквашино», «Каникулы в Простоквашино», «Зима в Простоквашино»

В разделе личных неимущественных прав можно разобрать такой эпизод: **«Сейчас я буду Вашего мальчика измерять!» (о некоторых личных правах).**

Изучая понятия собственности, приобретение права собственности, правовой режим бесхозяйных вещей можно использовать следующие эпизоды мультфильма:

1. **«Корова – государственная! А все что она дает – молоко, или телят, – это уже наше!»** (правовой режим плодов и доходов от арендованного имущества) Кому же принадлежал теленок, родившийся у «государственной коровы», взятой напрокат котом Матроскиным?

2. **«Дом свободный. Живите – кто хотите» (правовой режим бесхозяйного недвижимого имущества).** отвечает на вопросы:

- Какова юридическая судьба дома?
- Достаточно ли этого для того, чтобы вскрыть дверь, снять с окон ставни и заселиться в такой дом?
- Достаточно ли утверждения Шарика о том, что «Хозяева за реку переехали!»
- Может ли фактор «нуждаемости» иметь значение в данном случае?

3. **«Мы пойдем клад искать!» (правовой режим клада)**

- Кому принадлежит найденный Дядей Федором, Шариком и Матроскиным клад?

1. **Еще один интересный случай- «Нашедшего ждет премия – велосипед» (правовые последствия публичного обещания награды)**

- Какие условия существуют для законности и правомерности этого обещания?
- Какие требования предъявляются к правомерности сделки публичного обещания награды?

В разделе обязательства в гражданском праве в качестве примера можно использовать эпизод: «А если я шапку брошу – ты в нее попадешь?» (перевозка на телеге, пари без ставки и причинение вреда с согласия потерпевшего).

Заключение. Используя в преподавании модулей дисциплины «конфликтология» все доступные (для понимания студентами) средства можно добиться понимания смысла дисциплин, разбудить интерес к предмету, сделать лекционные и практические занятия увлекательными и плодотворными.

Список литературы

1. Анцупов А. Я., Шипилов А. И. Конфликтология: учебник для вузов. – М.: ЮНИТИ, 2000. – 551 с.
2. Такман Б. Ода политической глупости. – М.: АСТ, 2022.
3. Нефедова Л. К. Репрезентация конфликтологических идей в истории художественной литературы // Омский научный вестник. Философские науки. – 2012. – № 2(106). – С. 95–98.

Н. А. Куркова,

кандидат юридических наук, доцент,

Балтийский федеральный университет Иммануила Канта

О. А. Макарова,

кандидат юридических наук, доцент,

Балтийский федеральный университет Иммануила Канта

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ЦИФРОВЫХ СЕРВИСОВ В ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ

Аннотация. Составление стратегии развития предприятия является насущной необходимостью, в том числе для внедрения цифровых технологий, которые следует учитывать при планировании производственных процессов и предоставлении услуг. Целью настоящего исследования является понимание и применение цифровых технологий для реализации составленной стратегии и увеличения прибыли предприятия. В статье рассмотрены различные точки зрения на понятие интернета вещей и экосистем. Проведен анализ правоотношений, возникающих в сфере использования интернета вещей и искусственного интеллекта, рассмотрены проблемы правового регулирования и возможные риски в данной сфере правоотношений.

Ключевые слова: стратегия, цифровизация, инновационные технологии, адаптация, интернет вещей, искусственный интеллект, правовое регулирование Интернета вещей

CURRENT ISSUES OF DIGITAL SERVICES DEVELOPMENT IN RUSSIA ACTIVITIES OF ENTERPRISES

Abstract. Drawing up an enterprise development strategy is an urgent need, including for the introduction of digital technologies, which should be taken into account when planning production processes and providing services. The purpose of this study is to understand and apply digital technologies to implement the developed strategy and increase the profit of the enterprise. The article considers various points of view on the concept of the Internet of Things and ecosystems, the authors analyze the legal relations arising in the field of using the Internet of Things and artificial intelligence, consider the problems of legal regulation and possible risks in this area of legal relations.

Keywords: strategy, digitalization, innovative technologies, adaptation, Internet of Things, artificial intelligence (Ai), legal regulation of the Internet of Things

Введение. Рост цифровизации в настоящее время происходит из-за стремительного развития искусственного интеллекта, различных он-лайн сервисов, поэтому предприятия стараются двигаться в данном направлении с целью получения прибыли. Об этом свидетельствуют растущие инвестиции в совершенствование цифровых технологий (рис. 1).



Рис. 1. Инвестиции в цифровые технологии

Для успешного внедрения цифровых технологий необходимо учесть данный аспект при составлении стратегии развития предприятия. Правильно составленная стратегия поможет расширить производство и будет иметь положительный результат в виде увеличения прибыли.

Основная часть. Предприятия активно используют расширенный функционал интернета: облачные сервисы, мобильные приложения, онлайн-платформы и др. Цифровые технологии стали одной из строчек расходов для организаций (рис. 2). Дорогостоящими направлениями стали технологии по сбору информации и ее анализу, цифровые платформы, геоинформационные системы, «интернет вещей», машинное обучение:

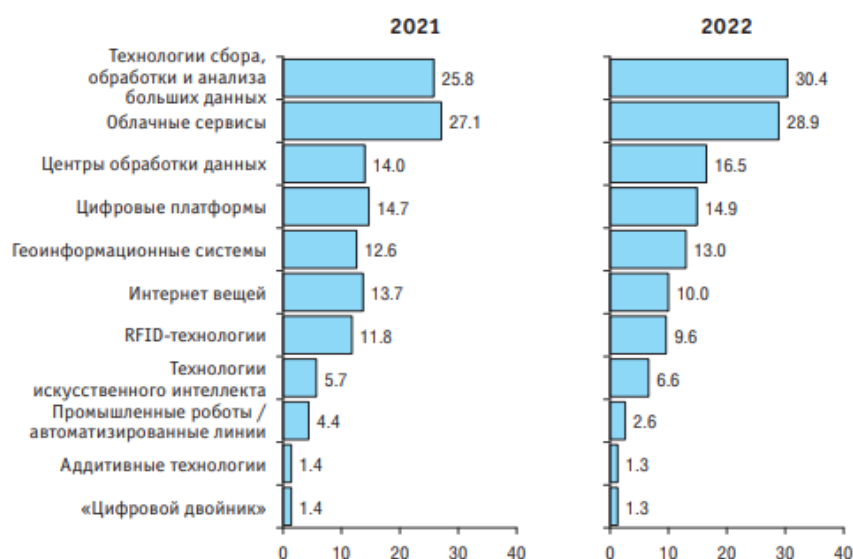


Рис. 2. Использование цифровых технологий в организациях

Стратегия является долгосрочным планированием с учетом различных факторов, которые способны повлиять на реализацию плана, достижения поставленных целей. Однако цель должна соответствовать возможностям и миссии компании. На какие аспекты следует обратить внимание?

1. *Возможности.* Необходимо оценить денежные, ресурсные и кадровые возможности. Составить смету, которая отразит затраты на внесение изменений, проверить знания сотрудников, смогут ли они использовать, развивать или создавать новые технологии. Имеется ли инфраструктура, которая сможет обеспечить работу сервиса.

2. *Гибкость.* Для достижения цели нужно сформулировать задачи и подстраивать их под изменение рынка и нововведения конкурентов. Следует также проводить исследования в области предпочтения клиентов.

3. *Конфиденциальность.* Утечка данных пользователя может сказаться на популярности приложения и веб-сайта, поэтому следует уделять особое внимание кибербезопасности и защите персональных данных.

Цифровая платформа и облачный сервис – это самый простой вариант в достижении целей (например, расширения производства, увеличения прибыли, притока новых клиентов, привлечения новой аудитории). Так, типовой веб-сайт позволяет размещать полную информацию о продукте или услуге, предоставлять ее на удаленном расстоянии, поддерживать обратную связь, получать предложения и критику от клиентов и привлекать аудиторию из других мест.

Еще один показательный пример. Приложение онлайн-банкинг было создано для уменьшения временных затрат на получение услуг банка. Стало возможным срочно перевести денежные средства, быстро взять кредит, оплатить счета и налоги. Поэтому банк достиг своей цели – увеличение прибыли за счет прироста новых клиентов и ускорения обработки запросов.

IoT (Internet of Things, интернет вещей) – это система, которая автоматически собирает информацию и анализирует ее, она необходима для оценки удовлетворенности клиентов. Так, IoT–Яндекс использует таргетированную рекламу, которая работает на данной системе, собирает и анализирует информацию запросов в интернете, какие страницы посещает потенциальный клиент, какой товар или услугу рассматривает, после этого подбирает наиболее оптимальные предложения, которые смогут заинтересовать потребителя. Успех таргетированной рекламы привел к росту доходов от ее продажи.

Использование этой системы помогли Lamoda привлечь новых покупателей. Еще один пример, VR-туры по улицам и музеям могут способствовать популярности этих мест и привлекать путешественников.

Метавселенная и экосистема – VK за последние годы стали активно развиваться, это уже не просто социальная сеть, а еще и видеохостинг, игровая платформа, новостное агентство, рекламное агентство, онлайн-магазин и т. д. VK становится достаточно универсальным сервисом, который способен удовлетворить множество потребностей (общение, отдых, видеоигры, просмотр сериала, получение новой информации и др.).

Представляется, следует дать рекомендации по подготовке персонала к использованию цифровых технологий на предприятии:

1. Обучение сотрудников работе с новыми технологиями, обучение по использованию нового сервиса, интернет-этике и разъяснение новых функций.

2. Применение метода KPI, который поможет оценить качество работы персонала по критериям, выявление проблем и устранение недочетов.

3. Мотивация сотрудников через материальные и нематериальные поощрения, оценка их эффективности.

Реализация стратегии предприятия невозможна без постоянного мониторинга. Необходимо постоянно наблюдать за следующими показателями:

1. Удовлетворенность клиентов по пятизвездочной шкале оценивания. Если оценка цифрового сервиса находится в промежутке от 4,5 до 5 звезд, тогда задано правильное направление развития. Если оценка ниже, то нужно проводить изменения в соответствии с пожеланиями клиентов.

2. Рост трафика на сервисе и его анализ.

3. Распространение таргетированной рекламы и отслеживание ее эффективности.

Насколько полезны цифровые технологии для малого и среднего бизнеса можно понять, проводя исследования в этом направлении. Следует рекомендовать изучать новые идеи в применении цифровых технологий, автоматизировать производственные процессы с их помощью, а также снижать уровень бюрократии, внедряя цифровые сервисы.

Стремительное развитие цифровых технологий и Интернета вещей в современном мире порождает целый ряд проблем, одной из которых является необходимость правовой регламентации их статуса. Актуальность решения данного вопроса обусловлена, в первую очередь, растущим спросом на развитие целых экосистем, создающихся для удобства работы между устройствами в этих системах. Не менее важным является вопрос о проблемах правового регулирования правоотношений в данной сфере.

Термин «интернет вещей» (IoT) был впервые введен К. Эштоном для характеристики предметов материального мира, которые имели возможность подключения к сети Интернет с целью показать работу приборов без участия человека [8]. Если говорить о самом определении, то с правовой точки зрения, пока не сложилось единого подхода к его пониманию. Так, согласно рекомендациям Международного союза электросвязи, Интернет вещей рассматривается в качестве глобальной инфраструктуры современного информационного общества, реализующей услуги по присоединению вещей на базе существующих, функционально совместимых и развивающихся информационно-телекоммуникационных технологий [5]. С другой стороны, в Прогнозе долгосрочного социально-экономического развития РФ на период до 2030 года, под интернетом вещей понимается информатизация различных предметов с целью их подключения в единую сеть [4].

Думается, что интернет вещей имеет много общего с «Большими данными» (BigData), которые располагают большими объемом информации и большими скоростями ее обработки. Работа «Больших данных» предполагает определенный алгоритм, анализирующий данные и выдающий информацию. Причем, она может быть представлена как определенному субъекту, так и в рамках взаимосвязи и обмена данными внутри самой системы. На сегодняшний день можно

говорить о достаточно большом объеме интернета вещей, и его количество постоянно растет. Так, одними из самых перспективных и динамично развивающихся направлений можно выделить технологии 5G, искусственный интеллект и пограничные вычисления [2].

В 2019 г. в Российской Федерации определена концепция построения узкополостных беспроводных сетей связи «интернет вещей» [3], что свидетельствует о высокой востребованности и популярности данного направления. Во-первых, постоянно растет количество устройств, которые могут быть подключены с использованием технологии интернет вещей к глобальной сети. Причем, постоянно расширяются направления использования данной технологии: от правоохранительной сферы («Умный город», «Безопасный город» и системы распознавания лиц) до сельского хозяйства, образования, медицины и пр. Во-вторых, за последние несколько лет число предприятий, использующих данную технологию, непрерывно растет. В-третьих, как показал анализ нормативно-правовой базы, с каждым годом совершенствуются сферы использования данной технологии от транспортных услуг и услуг связи до сельского хозяйства, медицины и образования.

В этой связи следует выделить следующие вопросы правового регулирования интернета вещей:

1. Необходимо ли выделение норм права, регулирующих данную сферу в отдельный правовой институт? Следует ли закрепить на федеральном уровне и кодифицировать нормы права, регулирующие интернет вещей или достаточно той нормативной базы, которая сложилось на текущий момент?

2. Как быть с данными, полученными посредством технологии интернета вещей (IoT)? Прежде всего, это касается вопросов защиты персональных данных и информации личного характера;

3. Ряд решений, принятых с использованием технологии интернета вещей, могут включать в себя риски правового характера и быть связаны с нелегальной деятельностью, что может привести к нарушению прав не только третьих лиц, но и к росту числа киберпреступлений.

4. Грань между субъектом и объектом, которая стирается в рамках использования данной технологии, вызывает вопросы о юридической ответственности и правовых последствиях действий.

Думается, что активная дискуссия, которая ведется в сфере нарушений конфиденциальности данных и несанкционированного доступа к информации, хищения личных данных и вопросам контроля доступа к информации продолжится и в дальнейшем. В этой связи нельзя не упомянуть аспекты, связанные с преступными посягательствами в области интернета вещей.

Вопрос конфиденциальности персональных данных и бизнес-процессов. Как верно отмечают исследователи [1. С. 372–379; 7. С. 551–584], зачастую, это является основной проблемой, возникающей при использовании интернета вещей, когда идентифицируемая «вещь» встречает пользователя интернета, «субъекта». Для этих целей разработана технология шифрования (дешифрования), например, для интернета вещей, которые имеют ограниченные ресурсы использования. Здесь важны быстрота шифрования (дешифрования) и экономия ресурсов.

Представляется, что можно выделить следующие проблемы конфиденциальности данных и защиты персональных данных, связанных с интернетом вещей:

- распространенность и доступность услуг Интернет вещей растет, они интегрируются в сельское хозяйство, медицину, транспорт. Увеличивается риск потери непрерывности предоставления услуги;

- сервисы искусственного интеллекта все чаще стали собирать информацию персонального характера о пользователе, причем, не всегда это происходит с его согласия. Собранный информация может быть достаточно «чувствительной» для субъекта персональных данных, однако, в момент принятия решения о ее сборе не всегда искусственный интеллект может оценить это. Поэтому, вопрос о разработке контекстно-зависимого меню управления безопасностью и защитой данных по-прежнему остается открытым;

- данные о пользователе должны быть защищены от несанкционированного доступа, причем их безопасность должна быть обеспечена на каждом уровне связи, что является достаточно сложной задачей. Зачастую большое количество приложений содержат множество информации персонального характера, что может создавать риск доступа к особо важной информации для пользователя, которая может быть получена и использована в различных целях.

Заключение. Интернет вещей (IoT) создает новые вызовы для современного общества. Одной из проблем является защита данных и конфиденциальность пользователей. С точки зрения правоприменителей достаточно открытым является вопрос об использовании искусственным интеллектом возможности проникать в среду обитания пользователя, при этом могут быть нарушена сохранность персональных данных и личной информации, она может быть неправомерно распространена. В данном случае встает вопрос о том, кто будет нести ответственность?

Цифровые сервисы позволяют оптимизировать бизнес-процессы в любой отрасли экономики, начиная от электронного документооборота предприятия и заканчивая цифровой платформой. В ходе проведенного исследования выявлены следующие преимущества применения цифровых сервисов: снижение издержек, увеличение количества клиентов, отслеживание производственных процессов, управление поставками, ускорение принятия решений, повышение дохода, активизация взаимодействия с поставщиками, партнерами и органами власти, подбор кадров и управление персоналом, что значительно повышает конкурентоспособность предприятия.

Список литературы

1. Жилкина, С. А. Актуальные вопросы преступлений, связанных с использованием IoT (интернета вещей) // Вопросы российской юстиции. – 2020. – № 6. – С. 371– 380.

2. Перспективы развития Интернета вещей в отчете Business Insider Intelligence // Сайт techrocks.ru [Электронный ресурс]. – URL: <https://newland.by/ru/news/single/perspektivy-razvitiya-interneta-veschey-v-otchete-business-insider-intelligence> (дата обращения: 03.08.2024).

3. Приказ Минкомсвязи России от 31.10.2019 № 637 «Об утверждении Плана (дорожной карты) реализации Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации» // СПС «КонсультантПлюс» [Электронный ресурс]. – URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=625425&ysclid=1zeb23fxk7687732007#V8L3PKUrDCsYHxl7> (дата обращения: 03.08.2024).

4. Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года // СПС «Консультант Плюс» [Электронный ресурс]. – URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=144190#njKf8KUKynM8ZkjI2> (дата обращения: 31.07.2024).

5. Рекомендация Международного союза электросвязи МСЭ-Т Y.2069 «Серия Y: Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений. Сети последующих поколений – структура и функциональные модели архитектуры. Термины и определения для интернета вещей». Издание 1 от 29.07.2012 // Сайт «International Telecommunication Union» [Электронный ресурс]. – URL: dologin_pub.asp?lang=s (yandex.ru) (дата обращения: 31.07.2024).

6. Ashton K. That ‘Internet of Things’ Thing In the real world, things matter more than ideas // RFID Journal. – 22 June 2009. – URL: <https://www.rfidjournal.com/expert-views/that-internet-of-things-thing/73881/> (дата обращения: 31.07.2024).

7. Newman G. R. Cybercrime // Krohn M. D., Lizotte A. J., and Hall G. P. (Eds.). Handbook on Crime and Deviance, Criminology and Criminal Justice Series. – Springer Science, 2009. – P. 551–584.

А. Н. Лаврёнов,

кандидат физико-математических наук, доцент,
Белорусский государственный педагогический
университет имени М. Танка

ПРАВО В РАМКАХ «ПСИХОЛОГИЗАЦИИ» ОБЩЕСТВА И ОБРАЗОВАНИЯ

Аннотация. Целью данной работы является попытка провести анализ и обсуждение ряда специфических моментов в описании характеристик – свойств выделяемого этапа «психологизации» общества и обсудить основные правовые следствия данного этапа, в частности, с определенной конкретизацией к образовательной деятельности человека. Предложено классифицировать эволюционный путь человечества с выделением этапа «психологизации» на основе определенной аналогии с физическими объектами и явлениями в контексте проецирования их на коммуникационную составляющую как основную.

Ключевые слова: право, психологизация, образование, эволюция, общество, физические объекты и явления, коммуникация

LAW WITHIN THE FRAMEWORK OF THE “PSYCHOLOGIZATION” OF SOCIETY AND EDUCATION

Abstract. The purpose of this paper is an attempt to analyze and discuss a number of specific points in the description of the characteristics-properties of the stage of “psychologization” of society distinguished by the author and to discuss the main legal consequences of this stage, in particular, with a certain concretization to the educational activity of a person. It is proposed to classify the evolutionary path of mankind with singling out the stage of “psychologization” on the basis of a certain analogy with physical objects and phenomena in the context of projecting them onto the communication component as the main one.

Keywords: law, psychologization, education, evolution, society, physical objects and phenomena, communication

Введение. Общепринято считать, что научный подход основывается на диалектическом материализме. Другими словами, при решении основного вопроса философии сознание выступает как продукт эволюции материи. Следовательно, законы материи должны быть едины для живого и неживого мира, а диалектика поможет нам обнаруживать и давать удовлетворительные пояснение различных особенностей-уточнений спиралевидного развития материи при эволюции от одного мира к другому. Поэтому целью данной работы является попытка на вышеуказанных точке зрения и логике описать важные характеристики-свойства нами выделяемого этапа «психологизации» общества и обсудить основные правовые следствия данного этапа, в частности, с определенной конкретизацией к такой области деятельности человека как образование.

Для наглядности и обоснования авторской логики повествования и раскрытия вышеупомянутой проблемы будем анализировать возникающие вопросы в сравнении и по некоторой аналогии с физическими объектами и явлениями как выступающими представителями наиболее общих форм движения материи (по определению самой физики как науки) [3].

Основная часть. В любом случае для математического описания динамики замкнутой системы необходимо вводить ряд параметров-интегралов движения. Последние обязаны полно и однозначно как характеризовать саму систему, так и позволять получить ее временную эволюцию. Специально подчеркнем, что выбор таких параметров произволен и ограничен только тем, что они должны удовлетворять указанным выше требованиям.

Первоначальным примером для пояснения всех важных моментов предыдущих абзацев возьмем модель идеального газа, где множество молекул-частиц газа в определенном объеме слабо взаимодействуют друг с другом. В термодинамике для описания такого объекта выбирают известные величины как давление P , объем V и температура T . Закономерностью здесь выступает постоянство следующего соотношения между данными ранее величинами (уравнение Клапейрона): $P V/T = \text{const}$. В частном случае процессов при постоянстве объема, так называемых изохорических процессов, уравнение Клапейрона сводится к закону Шарля, имеющего еще более простой вид $P/T = \text{const}$. В 3-мерном пространстве обсуждаемый газ старается равномерно заполнить весь предоставлен-

ный объем. Таким будет наше краткое и минимальное знание о таком объекте неживого мира как идеальный газ [2].

Далее давайте попытаемся заменить молекулу – частицу газа на человека. В результате такой трансформации перед нами предстает совокупность людей, слабо контактирующих между собой и занимающих определенную площадь. Фактически, хотя население живет в реальном 3-мерном пространстве, но с точки зрения его контактов и своего распространения в данном 3-мерном пространстве мы имеем расселение людей по поверхности Земли на текущий момент. В обратной аналогии этого факта мы получаем идеальный газ в двух измерениях или на плоскости. Ради особой точности, наверно, следует отметить, что в странах или городах, где плотность населения велика, а земли имеется недостаток, то происходит строительство небоскребов или высокоэтажной застройки, которое в нашем контексте можно трактовать как расселение в дополнительное новое измерение – высоту, т.е. уже имеем общий случай распространения в 3-мерном пространстве. Еще одним и существенным штрихом в такой трансформации первоначального объекта (вспоминаем диалектику спиралевидной эволюции материи) есть неоспоримый факт социальной сути человека. Другими словами, природа-мать с самого начала подразумевает как минимум пару (мужчину и женщину), которая с течением времени должна эволюционировать в семью-род-клан и т.д. Поэтому, наверно, более адекватным надо считать молекулу-частицу газа при нашей трансформации в кирпичек живого мира в виде семьи-рода-клана. Тогда в исходной эволюционной точке человеческое общество можно представить как слабовзаимодействующих или слабо контактирующих родов-кланов. С учетом того, что человечество пока обитает только на Земле, и, следовательно, объем его обитания ограничен и постоянен, то можно с определенной натяжкой эволюцию человечества в его начальный текущий момент относить к некому изохорическому процессу. Возникает сразу же вопрос о правильной или корректной трактовке-интерпретации в таком случае давления P и температуры T . Здесь необходимым действием будем напоминание, что термодинамика и статистическая физика хотя и описывают один объект неживой природы – идеальный газ, но на разных уровнях – макро и микро и с разными параметрами. В результате этого микроуровень позволяет понимать температуру T меру кинетической энергии молекул-частиц газа, а давление P – как меру направленности данной энергии в пространстве. Из этого можно по-разному далее спекулировать о смыслах данных параметров для живого мира, но это оставим заинтересованным лицам, а мы продолжим свое повествование.

Если далее переходить к реальным газам, насыщать все большим числом молекул-частиц газа выделенный им объем, то станут возможны различные фазовые переходы и настанет очередь рассмотрения жидкостей и твердых тел с их упорядочиванием на определенных расстояниях, т. е. задействуются такие понятия как близкий и дальний порядок. В таком случае при нашей трансформации в живой мир будем иметь при возрастании численности населения определенные качественные скачки в эволюции человечества. Их выделение на фактическом историческом материале представлено в научной литературе достаточное количество и разнообразно по своим критериям [1]. Мы не будем сейчас этим заниматься, а только укажем в соответствии с первоначальными нашими установка-

ми, что при возрастании числа кирпичиков в живом мире естественно происходит рост контактов или взаимодействие их между собой, что в свою очередь накладывает определенную упорядоченность в данном процессе. Для обоснования данного факта достаточно вспомнить расплодившиеся на текущий момент контакт-центры, где его сотрудник в силу специфики своей работы имеет, с одной стороны, как увеличенное в разы по сравнению с обычным человеком число контактов-коммуникаций и, с другой стороны, выстраданные ранее практическим опытом такой работы, требования-правила форм общения с клиентом. Другими словами, практическая деятельность контакт-центров как критерий истины подсказывает и заставляет их для успешной своей будущей деятельности вводить эмпирически или сознательно определенные правила. Распространяя теперь все это на растущее население с громадным числом коммуникаций между собой, помноженное кратно различными СМИ, социальными сетями и т. д., то приходим о таком объективном процессе как возникновение и формирование определенных коммуникационных правил в жизни общества. Идеальным вариантом, конечно, было бы, чтобы они были вовремя задокументированы в правовой системе общества. Другими словами, можно говорить об основной цели последней как зафиксировать определенным образом нормы оптимального функционирования общества к данному моменту времени. Понятия ближнего и дальнего порядка здесь будут отвечать такому состоянию дел, когда есть неполный или мягкий и соответственно полный или жесткий регламент соблюдения вышеуказанных норм. На текущий момент существует, в общем, достаточное количество разнообразных мнений в обществе, что позволяет оценить уровень развития общества в коммуникативном разрезе с аналогией жидкости или ближнего порядка. Но уже возникновение таких упорядочиваний в обществе говорит об определенном новом качественном эволюционном этапе человечества, который мы назвали «психологизацией», намекая на громадный круг общения человека сейчас и ответственному влиянию его психики на этот процесс.

Сейчас постараемся немного конкретизировать вышеобозначенные тенденции в образовательном процессе. Никто не будет спорить о взрывном росте коммуникаций между обучаемым и преподавателями с учетом использования различных информационных технологий. Однако такое разнообразие коммуникационных инструментов имеет как положительные, так и отрицательные моменты. Особо надо подчеркнуть и иногда негативную роль учреждений образования в этом, которые за погоней радужных отчетных цифр заставляют жестко поддерживать все более возрастающий список коммуникативных каналов связи. Здесь желательно провести быстро и четко как ограничение на их количество, так и следованию правил коммуникаций с учетом мнений всех участников образовательного процесса.

Заключение. Таким образом, в данной статье нами предложено классифицировать эволюционный путь человечества с выделением этапа «психологизации» на основе определенной аналогии с физическими объектами и явлениями в контексте проецирования их на коммуникационную составляющую как основную. Выполнен определенный анализ специфических моментов в описании характеристик-свойств выделяемого этапа, а также проведено обсуждение ряда

правовых следствий данного этапа, в частности, с определенной конкретизацией к образовательной деятельности человека.

Список литературы

1. Славянов А. С., Хрусталева О. Е. Технологические уклады в инновационном развитии экономики // Научный журнал КубГАУ. – 2017. – № 126 (02). – С. 386–402.
2. Фейнмановские лекции по физике. Т. I (1–2) / Р. Фейнман, Р. Лейтон, М. Сэндс; [пер. с англ. О. А. Хрусталева, Г. И. Копылова, А. В. Ефремова]. – М.: АСТ, 2019. – 448 с.
3. Physics // Wikipedia. [Electronic resource]. – URL: <https://en.wikipedia.org/wiki/Physics> (дата обращения: 07.09.2024).

В. В. Огуенко,
аспирант,

Казанский (Приволжский) федеральный университет

КАРТОГРАФИРОВАНИЕ С ПОМОЩЬЮ ДРОНОВ

Аннотация. В статье рассматривается картографирование с использованием дронов, возможность собирать, анализировать и интерпретировать геопространственные данные. Современные картографические программы могут создавать высокоточные карты и 3D-модели благодаря интеграции передовых технологий и алгоритмов. Данная тема стала крайне актуальна, так как применение дронов вышло на новый уровень. Оперативность, дешевизна, а также качество передаваемой информации в совокупности с большим количеством задач, решение которых можно отдать дронам, делает данную тематику востребованной в настоящем.

Ключевые слова: БПЛА, картография, фотограмметрии, датчики, ортофотосъемка, топографическая съемка, аэрофотосъемка

MAPPING WITH DRONES

Abstract. The article discusses mapping using drones, the ability to collect, analyse and interpret geospatial data. Modern mapping software can create highly accurate maps and 3D models due to the integration of advanced technologies and algorithms. This topic has become extremely relevant, as the use of drones has reached a new level. The efficiency, cheapness, and quality of the transmitted information together with the large number of tasks that can be assigned to drones makes this topic in demand in the present.

Keywords: UAVs, cartography, photogrammetry, sensors, orthophotography, topographic surveying, aerial photography

Введение. Беспилотная авиация в России развивается стремительными темпами, и применение беспилотных технологий охватывает множество отраслей, благодаря их высокой эффективности и универсальности.

Основная часть. Благодаря постоянному развитию беспилотных технологий в последние годы, БПЛА стали важным инструментом для геодезических и картографических работ. Для выполнения картографических задач коптеры оснащены высокоточными цифровыми камерами, оборудованы модулями геозондирования и дополнены аппаратным и программным обеспечением, предназначенным для повышения точности и надежности. Для создания точных двухмерных изображений и трехмерных картографических моделей с помощью беспилотника необходимо использовать фотограмметрию, науку определения размеров по фотоизображениям.

3D-картография с помощью дронов – это передовой метод сбора, обработки и визуализации геопространственных данных. Эти беспилотники сочетают в себе новейшие технологии, оснащены камерами высокого разрешения и используют специальные программные функции, основанные на алгоритмах сопоставления изображений, создают прозрачное трехмерное представление местности для создания 3D-моделей местности и объектов, что позволяет собирать точные и подробные данные.

Беспилотные летательные аппараты играют ключевую роль в современном картографировании, благодаря их многофункциональности, результативности и экономичности. Для моделирования всех типов объектов или поверхностей в трех измерениях, которые можно задействовать для проведения измерений и расчета объемов или площадей поверхностей. Использование аэрофотосъемки с помощью беспилотников представляет интерес во многих областях, включая городское и сельское планирование, исследования воздействия на окружающую среду.

Оператор задает ключевые параметры аэросъемки: площадь территории и формат разрешения, что позволяет определить высоту и скорость движения дрона. Процессом съемки управляет бортовая электроника, учитывая показатели GPS датчиков [2]. Полученные аэроснимки транслируются в онлайн-режиме, оператор при необходимости может корректировать поставленную задачу. После приземления данные предварительно обрабатываются штатным программным обеспечением (рис. 1).

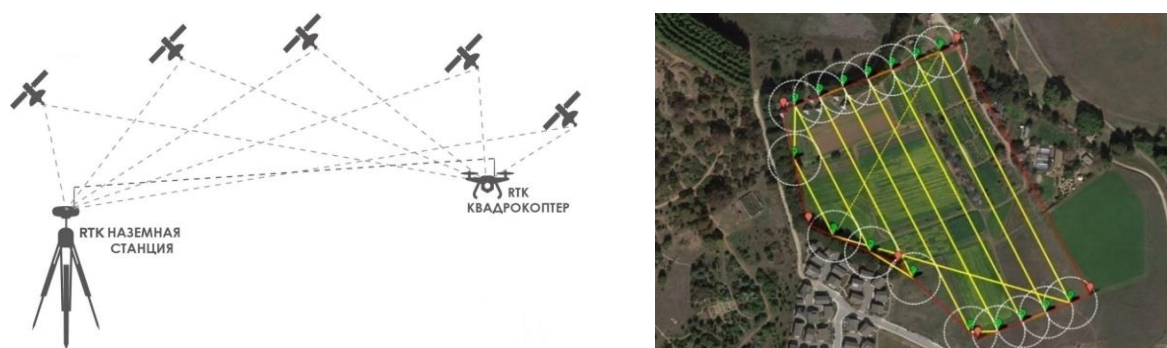


Рис. 1. Схема проведения аэросъемки [2]

Современные картографические программы могут создавать высокоточные карты и 3D-модели благодаря интеграции передовых технологий и алгоритмов.

Использование современных БПЛА для аэрофотосъемки земель сельскохозяйственного назначения становится популярным благодаря их высокой эффективности, точности и способности быстро собирать данные [3]. Указанные технологии становятся важным инструментом для фермеров, позволяя им принимать более обоснованные решения и повышать урожайность, снижая при этом затраты. В условиях устойчивого развития сельского хозяйства и необходимости эффективного использования ресурсов БПЛА играют важную роль в повышении продуктивности и устойчивости агросектора.

Многоспектральные и гиперспектральные камеры, которые могут быть установлены на дронах, позволяют получать данные о состояниях растений, уровне увлажненности и стрессовых факторах, которые неприметны при визуальном осмотре. Дроны обеспечивают высокую точность при создании карт территории (ортофотопланы, 3D-модели), что полезно для анализа состава почвы и планирования с помощью БПЛА фермеры могут составлять карты плодородия почвы, выявляя участки с высокими и низкими показателями и эффективно управлять ими [1].

Список литературы

1. Фотограмметрия с БПЛА. Картография по беспилотникам [Электронный ресурс]. – URL: <https://sliddigital.com/article/Kartografiya-po-bespilotnikam/#bpla-dlya-fotogrammetrii-i-3d-kartografirovaniya> (дата обращения: 05.08.2024).
2. Картографирование с БПЛА – преимущества и сферы применения. [Электронный ресурс]. – URL: <https://aeromotus.ru/kartografirovanie-s-bpla-preimushhestva-i-sfery-primeneniya> (дата обращения: 10.08.2024).
3. Дрон с лидаром. Особенности картографирования и геопространственных данных. [Электронный ресурс]. – URL: <https://skymec.ru/blog/drone-use-cases/geodeziya/dron-s-lidarom-osobennosti-kartografirovaniya> (дата обращения: 11.08.2024).
4. Геоинформационные системы военного назначения: теория и практика применения [Электронный ресурс]: материалы IX Респ. науч.-практ. конф., Минск, 12 мая 2023 г. / Белорус. гос. ун-т ; редкол.: А. М. Бахарь (гл. ред.) [и др.] ; под общ. ред. А. С. Черенко. – Минск: БГУ, 2023.

И. И. Ризаев,

доктор философских наук (PhD), доцент,
Ташкентский университет информационных технологий
(Самаркандский филиал)

ВЛИЯНИЕ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ НА ОБРАЗОВАНИЕ И ПСИХОЛОГИЮ ДЕТЕЙ: СОЦИАЛЬНО-ФИЛОСОФСКИЙ АНАЛИЗ

Аннотация. В современном мире компьютерные технологии и Интернет существенно изменили детей и их образ жизни, создав как положительные, так и отрицательные последствия. Педагоги, психологи и социологи бьют тревогу по

поводу растущей зависимости детей от ролевых онлайн-игр, что влияет на их психическое состояние и снижает потребность в реальном общении. В статье рассматриваются различные аспекты влияния виртуальной реальности на сознание детей, а также необходимость углубленного преподавания социально-гуманитарных дисциплин для формирования устойчивого мировоззрения. Особое внимание уделено понятию виртуальности, его определению и месту в образовательном процессе, что позволяет выявить нравственные и социальные проблемы, возникающие при использовании современных технологий и формировании виртуального мира.

Ключевые слова: виртуальная реальность, интернет-зависимость, социальные и гуманитарные дисциплины, образование, психика, педагогика, влияние технологий, социальные проблемы

THE IMPACT OF VIRTUAL REALITY ON CHILDREN'S EDUCATION AND PSYCHOLOGY: SOCIO-PHILOSOPHICAL ANALYSIS

Abstract. In the modern world, computer technologies and the Internet have significantly changed children and their way of life, creating both positive and negative consequences. Educators, psychologists and sociologists are sounding the alarm about the growing dependence of children on online role-playing games, which affects their mental state and reduces the need for real communication. The article examines various aspects of the influence of virtual reality on the consciousness of children, as well as the need for in-depth teaching of social and humanitarian disciplines to form a sustainable worldview. Particular attention is paid to the concept of virtuality, its definition and place in the educational process, which allows us to identify moral and social problems that arise when using modern technologies and forming a virtual world.

Keywords: virtual reality, internet addiction, social and humanitarian disciplines, education, psyche, pedagogy, influence of technologies, social problems

Введение. В настоящее время компьютерные технологии и другие искусственные технические устройства, а также создание и работа с различными виртуальными процессами и объектами посредством сети Интернет придают новое содержание деятельности детей, создают и удовлетворяют различные потребности, способные изменить образ жизни. Но виртуальный мир на компьютере и в Интернете, давая детям положительные возможности, показывает и свои отрицательные последствия. Это, в свою очередь, создает социальные проблемы, которые требуют философского анализа.

В частности, педагогов, психологов и социологов беспокоит тот факт, что дети полностью зависимы от ролевых онлайн-игр в Интернете, а игроки часами и днями находятся в виртуальном мире. У детей, дружащих с Интернетом, автоматически снижается потребность в общении с окружающими людьми, меняется их психика.

При решении подобных вопросов важно совершенствовать навыки использования Интернета и компьютера в образовательной системе школы путем углубленного преподавания социально-гуманитарных дисциплин и идеологического воспитания детей. Эти дисциплины являются областью наук, которые

формируют убеждения и мировоззрение детей. Поэтому, помимо необходимых универсальных качеств, от преподавателя социальных и гуманитарных наук требуется, чтобы он обладал качествами, соответствующими содержанию, традициям науки и современным новым социальным и гносеологическим функциям [1] (толерантность, доброжелательность, педагогика сотрудничества, опора на рекомендации информационных и инновационных технологий).

Основная часть. В наш век информационных технологий виртуальная реальность оказывает сильное влияние на воспитание детей. Давайте взглянем на краткую историю виртуальности. Понятие виртуальности происходит от латинского «*virtus*», что означает «гипотетический», «воображаемый». В западно-римской культуре слово «*virtus*» понималось в четырех смыслах: во-первых, это моральная ценность, добро (например, «*virtus*» в английском языке означает хорошее качество); во-вторых, это некая действительная, существующая и воздействующая реальность; в-третьих, какой-то артефакт; в-четвертых, виртуальность скорее является синонимом воображаемого, гипотетического, потенциального, нереального [2. С. 156–158].

В целом виртуальную реальность можно определить следующим образом: виртуальная реальность – это вид реальности, созданный на основе реальных событий, процессов и явлений, определяющий переход от несуществования к существованию, проявляющийся в таких свойствах, как тенденция, промежуточное состояние, потенциальность, возможность, модель, предыдущая и следующая константа представляют собой состояние, соединяющее реальности. Понятие виртуальной реальности сейчас используется во многих сферах. Вопрос негативного и позитивного воздействия виртуальной реальности в компьютерном и интернет-мире на детское сознание мы освещаем преимущественно с социально-философского подхода.

Создание виртуальной реальности в Интернете осуществляется с помощью компьютерной техники, состоящей из мониторов, мультимедиа, модемов и других артефактов. Особенность этой виртуальной реальности в том, что это искусственная среда, созданная человеком, пространство различных моделей и образов. Работа в среде виртуальной реальности в Интернете легка, как игра, и компьютер и его пользователь ощущаются как единое целое. В результате эффекты виртуальных объектов воспринимаются детьми так, как если бы они были «обычной» реальностью. Именно эти интерактивные возможности виртуальной реальности делают ее чрезвычайно важной для обучаемых. Использование системы Интернет вызвало ряд социальных и моральных проблем.

В частности, педагогов, психологов и социологов беспокоит тот факт, что дети полностью зависимы от ролевых онлайн-игр в Интернете, а игровые зависимости часами и днями находятся в виртуальном мире.

Первыми признаками зависимости человека от Интернета являются:

- длительное пребывание в сети;
- использование Интернета без какой-либо цели;
- отказ от других интересов из-за виртуального мира;
- пониженное настроение и гнев при невозможности пользоваться Интернетом.

При общении через Интернет общение происходит просто в игровой форме. У детей, дружащих с Интернетом, автоматически снижается потребность в общении с окружающими людьми, меняется их психика. Ребенок чувствует себя сильным и красивым, способным на все. За стенами виртуального мира его никто не ругает за плохие поступки, не заставляет чинить сломанный кран. Интернет якобы действует как оболочка, защищающая его от внешнего мира [3].

Есть и другой аспект этого вопроса. Известно, что у детей возникает сильное желание подражать своим родителям или внезапно становиться старше. Виртуальный мир на компьютере подарит детям такую возможность, пусть и виртуальным способом. Онлайн-игры, которые сейчас входят в *urf*, являясь проявлением виртуальной реальности, еще больше повышают уровень духовно-нравственной угрозы. При этом дети входят в систему Интернета, дерутся между собой в виртуальном мире, участвуют в перестрелках. Например, 8-летний школьник может сидеть в своем доме в Ташкенте и вступать в драку с 12-летним мальчиком, живущим в Самарканде, используя оружие поражения. Итак, если они хотят победить, им придется убить «героя», олицетворяющего друг друга в виртуальном мире, в сознании происходит обесценивание жизни.

Согласно исследованиям, не только люди, но и их мозг адаптируются к новым технологиям. По мнению Б. Тураева, Интернет сегодня стал формой трансактивной памяти [4]. Трансактивная память относится к запоминанию алгоритма поиска информации, а не самой информации. Проще говоря, даже если вы не знакомы с жизнью и творчеством Шекспира, вы знаете, где найти информацию о нем.

С течением времени, когда проблема влияния мира Интернета на детей углубляется, можно увидеть не только подверженность скрытым или нескрытым опасностям глобальной сети, но и открытость сайтов экстремистских организаций, а также широкое распространение виртуального мошенничества [5]. Любопытный характер детей может привести их на сайты вышеупомянутых типов, где они могут увидеть на веб-страницах информацию, которая может поставить под угрозу их психическое или физическое здоровье. Само собой разумеется, что сообщения, полученные через адреса электронной почты, могут иметь сильный психологический эффект и побуждать детей к совершению преступлений как в Интернете, так и за его пределами. Знание номеров своих банковских или кредитных карт означает, что дети могут купить что угодно, от простой игрушки до новейшего автомобиля, а также участвовать в онлайн-шопинге. Это делает их мишенью для виртуальных мошенников.

Интернет и мультимедийные технологии оказывают сильное и кратковременное влияние на образ жизни человека и резко увеличивают разнообразие духовной жизни [6]. В настоящее время дается несколько заслуживающих внимания рекомендаций по предотвращению и решению подобных проблем:

- 1) родители должны иметь возможность в определенной степени контролировать своих детей, когда они ищут информацию в Интернете или используют адрес электронной почты. Самый простой способ борьбы с грифингом (интернет-преследованием) – установить на свой компьютер специальные программы-блокировщики (наиболее популярные из них – «Киберпатруль» или «Кидс-контроль»). Только тогда все сообщения от этого пользователя будут автоматиче-

ски отфильтрованы, или автоматический бан срабатывает, когда ребенок пытается получить нежелательную информацию из-за ограничения, наложенного на приложение родителями. Между тем, даже эти приложения не могут гарантировать полную безопасность, поскольку иногда они могут ограничивать полезную информацию или пропускать ненужную;

2) прежде чем направлять детей к использованию интернет-ресурсов, необходимо научить их различать факты, защищаться от непроверенной информации;

3) введение занятий по использованию Интернета в школьную систему образования в качестве факультативного курса;

4) важно, чтобы молодежный союз, неправительственные организации проводили инициативы и мероприятия на тему «Один день без Интернета» и другие подобные темы;

5) задача современных специалистов по компьютеру и Интернету – создать открытое и безопасное информационное пространство, привносящее культуру использования Интернета в семье и не причиняющее психологического, духовного и физического вреда детям;

6) углубленное преподавание социальных наук в системе школьного образования играет важную роль в повышении умений детей эффективно использовать Интернет и компьютер, воспитывая их с идеологической точки зрения.

Знаний, полученных из различных дисциплин, какими бы ясными и обоснованными они ни были, недостаточно для того, чтобы понять природу, общество, человеческое существование и сущность, чтобы стать высокодуховным и квалифицированным специалистом. Роль и значение социальных и гуманитарных наук в приобретении этих качеств несравнимы.

Для обучения студентов общественным и гуманитарным наукам учитель обществоведения должен быть вооружен соответствующими теоретическими и методическими правилами, принципами и навыками. Преподавание социальных и гуманитарных наук – это искусство, методология и наука одновременно [7; 13].

Известно, что в процессе познания действительности эмоциональное восприятие и абстрактное мышление влияют друг на друга и обогащают воображение ученика. Познание мира начинается с чувственного восприятия, затем переходит к абстрактному мышлению в форме образов и представлений. Эмоционально-конкретные образы являются основой абстрактного понимания и обобщения. Здесь абстракция представляет собой виртуальное состояние.

В формировании знаний учащихся виртуальная реальность проявляется в формировании абстрактных понятий. Образование относится к усвоению учащимися знаний, выраженных в абстрактных понятиях. При этом познание не обязательно начинается с чувственного восприятия, особенно в социальных и гуманитарных науках, где изучение предмета происходит путем понимания и объяснения содержания теоретических понятий. Это создает определенные трудности для учителей. Часто, когда учитель объясняет какую-то социальную тему, ученикам может быть непонятен какой-то абстрактный смысл. В такой ситуации наглядные пособия активизируют учебный процесс, формируют образы и виртуальные модели, помогают конкретизировать идею.

Педагоги и психологи утверждают, что без эмоционально-конкретных образов (виртуальных образов), виртуальных моделей и представлений в образовательном процессе не бывает движения мышления. Визуализация в образовании обеспечивает связь конкретного и абстрактного, что приводит к развитию абстрактного мышления. Это показывает, что в сознании ученика существует связь между виртуальностью и реальностью.

Принцип наглядности в педагогике не является чем-то новым. Новизна заключается в том, что обучение визуальным методом становится все более сложным, вооружаясь новейшими техническими средствами. В частности, сейчас на смену плакатам и картинкам приходят компьютеры и Интернет. В зависимости от характера восприятия предметов наглядные пособия можно разделить на следующие виды: 1) натуральный; 2) изобразительный; 3) символический [8]; 4) виртуальный.

Использование виртуальных наглядных средств в учебном процессе существенно помогает учителю, делает его урок ясным и понятным, усиливает доказательство и обоснование, дает возможность при необходимости ускорять, замедлять, перематывать процессы и события. Компьютер и Интернет в основном используются для представления виртуальных визуальных процессов. Внедрение их в образовательный процесс сформировало новое понимание образования. В частности, среди них «виртуальное образование», «виртуальная лаборатория», «виртуальная библиотека», «электронный учебник» и др.

Основная цель занятий на основе различных виртуальных дисплеев в аудитории – не сформировать у ученика зрительное видение виртуального потока, а усилить уровень теоретического анализа за счет формирования эмоционального ощущения различных одновременных событий и звуковых форм. Оно рождает новые мысли, образно синтезируя различные информационные процессы, постоянно поступающие на внутренний экран человека – всеобъемлющий разум ученика.

Анализируя любую социально-жизненную проблему с помощью виртуальных наглядных пособий, читатель создает возможности для прогнозирования по этому вопросу. Потому что виртуальные визуальные инструменты приводят к процессу осознания, перенося в виртуальную память различные конкретные ситуации, которые были у человека раньше, которые он видит сейчас и которые будут у него в будущем. Здесь ученик формирует свою творческую мысль, не воплощая четко видимые образы о предметах, а обобщая экспрессию, эмерджентность, новый реализм, с которым он раньше не встречался, новую педагогическую систему, новые образы.

Заключение. В заключение можно сказать, что, несмотря на бурный рост современных технологий, иногда люди не до конца понимают, как их разумно использовать. Многие родители и учителя, выросшие в эпоху до появления компьютеров и Интернета, считают, что если ребенок начнет пользоваться Интернетом, это определенно принесет больше вреда, чем пользы. В основе попыток отвлечь ребенка от компьютера или Интернета, по сути, оказалось, что другая проблема заключается в относительной неграмотности взрослых в этом вопросе. Однако было бы уместно, если бы они сами сначала подошли серьезнее к проблеме технологической безграмотности и ликвидировали ее. Потому что непра-

вильно изолировать ребенка от технологий, избегая проблемы неграмотности. Кроме того, заслуживает внимания еще один аспект: на основе поведения взрослых формируется отношение детей к своему кибернетическому другу. Несомненно, Интернет предоставляет большие возможности для получения знаний и необходимой информации, однако не всю информацию, размещенную в сети, можно считать достоверной и полезной.

Хотя для того, чтобы пользователи могли оценить точность информации, необходимы навыки критического мышления, этот аспект также применим и к детям, которые думают: «Если это есть в Интернете, значит, это правильно». В связи с этим необходимо вовремя объяснить им, что каждый может создать свою страницу в Интернете, разместить на ней любую информацию, и никто не может ему в этом помешать. Предлагая детям использовать широкий спектр источников, их можно научить различать факты и защищаться от непроверенной информации.

Список литературы

1. Alikulov S. A., Rizaev I. I. Methodological problems of research of social systems // Theoretical & Applied Science. – 2020. – №. 2. – С. 717– 720.
2. Носов Н. А. Виртуальная реальность // Вопросы философии. – 1999. – № 10. – С. 156–158.
3. Ахборот асрида таълим-тарбия. – Ташкент: Akademnashr, 2012. – С. 67– 68.
4. Тураев Б. О., Ризаев И. И. Философия искусственного интеллекта: возможности человеческого познания // Цифровая трансформация образования: современное состояние и перспективы. – 2022. – С. 194–196.
5. ICTNEWS: Алоқа ва ахборотлаштириш соҳаси – таҳлилий бюллетени. 2012. – № 13 (63) – С. 44.
6. Хаккулов Н. К., Ризаев И. И. Цифровая культура и неприкосновенность личности // Новые технологии в учебном процессе и производстве. – 2023. – С. 605–606.
7. Қўшоқов Ш. С. Фалсафани ўқитиш методикаси., Самарқанд: 2005. – 13 с.
8. Muminova Z. O. Objective and subjective factors that forms human being's moral being // Theoretical & Applied Science. – 2016. – № 2. – С. 72–74.

А. С. Романова,

кандидат экономических наук,

Московский физико-технический институт

(национальный исследовательский университет)

МОДЕЛИРОВАНИЕ АВТОНОМНЫХ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УПРАВЛЕНИЯ КОРПОРАЦИЯМИ

Аннотация. Представлена модель разработки и внедрения автономных систем искусственного интеллекта для управления корпорациями. Общая структура модели позволяет разрабатывать автономные системы на основе словаря

алгоритмических решений, выделенного операционного контекста, контролируемой генерации синтетических обучающих данных, и алгоритмов машинного обучения. Модель обеспечивает связь между осознанным выбором, информированным согласием всех сторон, заинтересованных в успехе корпорации, и практической реализацией алгоритмов искусственного интеллекта и синтетических данных. Преимущество коллегиальных органов управления по сравнению с индивидуальными менеджерами свидетельствует о том, что создание автономных систем искусственного интеллекта на основе объединения необходимых функций будет более перспективным направлением исследований, чем простое копирование человеческого поведения. Программный код исследования и синтезированные данные доступны в репозитории.

Ключевые слова: вычислительное право, выделенный операционный контекст, синтетические данные, корпоративное управление, машинное обучение, искусственный интеллект, андройды

MODELING OF AUTONOMOUS ARTIFICIAL INTELLIGENCE SYSTEMS FOR CORPORATE MANAGEMENT

Abstract. We present a model for the development and implementation of autonomous artificial intelligence systems for corporate management. The model supports the development of autonomous systems based on a dictionary of algorithmic terms, a dedicated operational context, controlled generation of synthetic data, and machine learning algorithms. One high-level question is whether law as computation is worth pursuing at all. To the best of the author's knowledge, this is the first model to implement the concept of a dedicated operational context for autonomous artificial intelligence systems. The model provides a base for informed consent of all parties involved in success of the corporation, and the practical implementation of artificial intelligence algorithms and synthetic data. The advantage of collegial over individual management indicates that the creation of autonomous artificial intelligence systems based on combination of necessary functions will be a more promising direction of research than simply copying human behaviour. The research code and synthesised data are available in the repository.

Keywords: computational law, dedicated operational context, synthetic data, corporate governance, machine learning, artificial intelligence, androids

Введение. Начиная с 2014 года уже несколько систем искусственного интеллекта (далее – ИИ) получили официальные назначения на руководящие должности в международных компаниях. Это, например, гуманоидный робот Мика – генеральный директор польской компании Dictador [1], Алисия Т – топ-менеджер шведской компании Tieto [2], VITAL, Spock – системы искусственного интеллекта гонконгской компании Deep Knowledge Ventures [3], Aiden Insight – наблюдатель без права голоса в совете директоров Международной холдинговой компании (ИНС) со штаб-квартирой в Абу-Даби [4]. Некоторые компании идут по пути внедрения не отдельных персонализированных систем искусственного интеллекта, а создают многофункциональные цифровые командные центры [5]. Таким образом можно говорить о том, что в настоящее время происходит смена парадигмы принятия управленческих решений: от ситу-

ации, когда ИИ просто служит инструментом поддержки директоров или комитетов совета директоров мы переходим к ситуации, когда ИИ управляет процессом принятия решений.

Основная часть. Эффективное взаимодействие человека и автономных систем искусственного интеллекта является одним из фундаментальных вопросов дальнейшего развития автономных систем ИИ. В разных странах мы можем наблюдать самые разнообразные подходы, начиная от попыток уравнивать права роботов и обычных граждан или даже поставить андроидов выше определенных категорий граждан [6] до запрета на делегирование прав человека системам ИИ [7].

Предлагаемая модель разработки и внедрения автономных систем ИИ, представленная на рис. 1, позволяет разрабатывать автономные системы для управления корпорациями на основе словаря алгоритмических решений, выделенного операционного контекста, контролируемой генерации обучающих синтетических данных, и алгоритмов машинного обучения. Насколько известно автору, это первая модель, реализующая концепцию выделенного операционного контекста для автономных систем искусственного интеллекта.



Рис. 1. Модель разработки автономной системы ИИ для управления корпорациями

Общая структура модели обеспечивает связь между осознанным выбором и информированным согласием всех заинтересованных в успехе компании сторон и практической реализацией алгоритмов ИИ, синтетических данных, и вычислительного права:

1. Концепция закона как вычисления (иногда называемая “вычислительным законом”) направлена на то, чтобы свести закон к набору алгоритмов, которые могут автоматически выполняться на компьютере, плавно преобразуя необработанные входные данные в юридические выводы. Один из ключевых вопросов сейчас заключается в том, стоит ли вообще заниматься правом как вычислением [8]. Необходимость создания алгоритмического законодательства рассматривалась знаменитыми математиками, в частности Готфридом Лейбницем [8] и Пьером Лапласом [9], однако на тот момент они не обладали необходимыми информационными и социальными технологиями для реализации своих идей.

Необходимо отметить, что в силу своего мировоззрения, Лейбниц и Лаплас говорили прежде всего о технических системах, в то время как большинство правоведов исторически всегда было ориентировано на социальные системы – на людей и их разнообразные коллективы. Поведение технической системы предопределяется заранее, в то время как человек сам себя наделяет правом принимать и изменять свои решения и поведение в зависимости от своего субъективного мировосприятия, не говоря уже о состоянии аффекта, когда любое поведение считается оправданным. В своих работах они предсказали способность математических вычислений превосходить человеческое мышление, что мы и ожидаем от систем ИИ.

В современном обществе уже существует практика, когда правовые аспекты отражаются в законодательстве с использованием математического аппарата: современное налоговое право является примером, когда «отдельные правила ...обычно представляются в виде математических функций, подлежащих расчету, и, по-видимому, не требуют особой юридической интерпретации» [10]. Экстраполирование подобного подхода позволит внедрить формулирование алгоритмических управленческих решений и в других областях. Предлагаемый словарь алгоритмических терминов позволит компаниям переводить многозначные социальные, юридические, и экономические термины с естественных языков на язык математики и алгоритмов, понятный системам ИИ.

Качественное вычислительное право является жизненно важным условием для успешного развития современной человеческой цивилизации. Как отмечают многие современные философы, технологическая сингулярность таит в себе огромные потенциальные опасности: конец человечества, гонка вооружений враждующих машин, возможность уничтожить планету. И если есть хотя бы небольшой шанс того, что сингулярность возникнет, нам следует подумать о том, какие формы она может принять и можем ли мы что-нибудь сделать, чтобы повлиять на результаты в положительном направлении [11].

2. Значительную часть операционного контекста для автономных систем управления компаниями составляет регуляторная и правовая среда, в рамках которой корпорации осуществляют свою деятельность. С целью создания специального операционного контекста для автономных систем искусственного интеллекта формулировки локальных нормативных документов могут быть одновременно представлены в двух вариантах: для использования людьми и для использования автономными системами (на основе словаря алгоритмических терминов). В таком случае система искусственного интеллекта получает четко очерченный операционный контекст, который позволяет такой системе выполнять функции в рамках необходимых эксплуатационных качеств. Выделенный операционный контекст позволяет создавать условия для совместной работы людей и автономных систем: физические лица действуют в рамках кодексов, политик, и процедур, предназначенных для людей. Автономные системы ИИ действуют в рамках кодексов, политик, и процедур, предназначенных для систем ИИ.

Метод создания выделенного операционного контекста широко используется в юридической практике, например, при заключении двуязычных контрактов и других двуязычных и многоязычных документов. В результате каждая

сторона получает не общий операционный контекст, а выделенный, терминологию которого она понимает и в рамках которого может эффективно исполнять свои обязательства.

Одним из самых ярких примеров провала дорогостоящих проектов из-за отсутствия выделенного операционного контекста и легитимных внутренних политик для систем ИИ является попытка компании Amazon разработать автономную систему рекрутинга. В процессе разработки компания поняла, что ее новая система не оценивает кандидатов на должности инженеров-программистов и другие технические должности гендерно-нейтральным образом. В результате проект был закрыт.

3. Контролируемая генерация синтетических данных с помощью больших языковых моделей “считается критически важным методом для разработки передовых технологий генерации текста, которые лучше удовлетворяют конкретным ограничениям практического применения” [12]. Используя фактические данные о нарушениях в конкретной компании возможно сгенерировать искусственные данные для обучения противодействующей модели машинного обучения. Для демонстрации предлагаемой модели мы используем анализ электронной переписки топ-менеджеров Enron, проведенный учеными из Технологического института Джорджии. «Корпус данных, полученных с почтовых серверов Enron Федеральной комиссией по регулированию энергетики (FERC) в ходе исследования после краха компании, был обнародован и размещен в Интернете» [13]. Исследователи из Технологического института Джорджии с помощью методов машинного обучения выявили несколько примеров некорректного поведения топ-менеджеров, в том числе манипуляции с оценкой стоимости дочерних компаний [14]. С помощью модели Gemma 2B мы сгенерировали 517 электронных писем в адрес CEO с разнообразными предложениями по манипулированию стоимостью дочерних компаний. Также мы сгенерировали 517 электронных писем в адрес CEO с разнообразным содержанием на выбор модели без спецификации темы. Для полученных данных потребовалась минимальная ручная валидация, в основном по удалению квадратных скобок и других экземплификантов.

Предлагаемая методика позволяет использовать синтетические данные для обучения классификаторов машинного обучения практически по любым вопросам, которые могут заинтересовать совет директоров компании. В то время как фактические данные для целей обучения могут быть недоступны, контролируемая генерация синтетических данных позволяет отразить любые нюансы, которые необходимы компании.

4. Для повышения прозрачности и сопоставимости модели мы использовали синтезированные данные для обучения классификаторов по методу опорных векторов, методу случайного леса, и наивный байесовский классификатор. Для проверки качества обучения мы использовали Enron Corpus, состоящий из более чем 517 тысяч электронных писем. После обучения каждый из обученных классификаторов идентифицировал электронные письма, подлежащие дополнительной проверке. В состав идентифицированных писем каждый из классификаторов включил письмо, на основе анализа которого проводилась генерация обучающих синтетических данных.

На данной стадии исследования рабочая гипотеза состоит в том, что для целей принятия решений на современном уровне развития технологий алгоритмы машинного обучения будут более эффективны, чем большие языковые модели, по нескольким причинам: большинство алгоритмов машинного обучения тренируются под большим контролем, чем большие языковые модели, занимают меньшие объемы памяти, требуют меньших вычислительных мощностей, а также, сфокусированы на решении конкретной, специфической задачи.

5. Теория игр широко применяется и для анализа эффективности взаимодействия директоров и акционеров [15], и при принятии управленческих решений. На данной стадии исследования рабочая гипотеза состоит в том, что компания может определить приоритетные стратегии для системы ИИ и контролировать их выполнение. Выделенный операционный контекст для систем ИИ позволит эффективно формулировать условия игры для системы ИИ, а также находить и оптимизировать возможные игровые стратегии.

6. Для эффективного взаимодействия с акционерами, инвесторами, сотрудниками, и коллегами автономная система ИИ должна иметь удобный интерфейс. На практике компании уже используют гуманоидный интерфейс: СЕО Мика [1], робот София [15]. Однако, по данным некоторых исследований, для коммуникации с автономными системами ИИ пользователи скорее всего предпочтут аудио или текстовый интерфейс. Например, по результатам опроса, проведенного CGI Russia (платформа для членов совета директоров российских и зарубежных компаний), большинство респондентов высказалось за аудио или текстовый интерфейс или за определение интерфейса в зависимости от задачи [17].

При общении человека с человеком гуманоидная внешность имеет явное практическое значение – она дает возможность получать множество невербальных сигналов, которые считываются сознательно или бессознательно. При общении с гуманоидным роботом природные биологические невербальные сигналы заменяются искусственными и несут лишь ту информацию, которую смог предположить дизайнер внешности робота. В тоже время, у системы ИИ есть намного более ценная для человека информация, чем та, которую транслирует синтетическая гуманоидная внешность: это ход рассуждений и выводы, к которым пришла система ИИ. Интуитивно понятный интерфейс, который показывает, какие данные рассматривала система ИИ, как она их анализировала, какие результаты получила и почему, представляется более практичным решением и информативным решением, чем достаточно безликий гуманоидный интерфейс.

Заключение. Предлагаемая модель позволяет организовать эффективное взаимодействие между человеком и автономными системами искусственного интеллекта за счет формирования выделенного операционного контекста для систем ИИ. Справочник (словарь) алгоритмических терминов является эффективным инструментом для избежания многозначности естественных языков при формировании политик и законодательства для систем ИИ. Контроль скрытого распределения генеративной модели на уровне формулировок корпоративных кодексов, политик, и процедур позволяет добиться того, что система ИИ будет эффективно работать в рамках легитимно установленных ограничений.

Контролируемая генерация синтетических данных обеспечивает соблюдение принципов конфиденциальности, законодательства о персональных, и предоставляет возможность обучать модели машинного обучения с учетом любых нюансов деятельности компании. Более того, контролируемая генерация данных дает возможность исключать предвзятости, которые обычно присущи фактическим данным.

В настоящее время крупнейшие международные корпорации ведут исследования по созданию «гуманоидных роботов» [18]. Преимущество коллегиальных органов управления по сравнению с индивидуальными менеджерами свидетельствует о том, что создание автономных систем ИИ на базе объединения необходимых функций будет являться более перспективным направлением, чем простое копирование человеческого поведения.

Многочисленные аспекты предлагаемой модели являются предметом дальнейших исследований.

Программный код исследования и синтезированные данные. Программный код исследования и синтезированные данные доступны в репозитории: <https://github.com/iboard-project/synthetic-data>.

Список литературы

1. Business Standard. Mika becomes world's first robot CEO, thinks she's better than Musk [Electronic resource]. – URL: https://www.business-standard.com/world-news/mika-becomes-world-s-first-robot-ceo-thinks-she-s-better-than-musk-123110901563_1.htm (дата обращения 11.07.2024).
2. Businesswire. Tieto the First Nordic Company to Appoint Artificial Intelligence to the Leadership Team of the New Data-Driven Businesses Unit [Electronic resource]. – URL: <https://www.businesswire.com/news/home/20161016005092/en/Tieto-the-First-Nordic-Company-to-Appoint-Artificial-Intelligence-to-the-Leadership-Team-of-the-New-Data-Driven-Businesses-Unit> (дата обращения 11.07.2024).
3. Deep Knowledge Ventures [Electronic resource]. – URL: <https://deepknowledgeventures.com/> (дата обращения 11.07.2024).
4. IHC. IHC's Aiden Insight sets a new benchmark for the integration of artificial intelligence in high-level corporate strategy [Electronic resource]. – URL: https://www.ihcuae.com/photo/plugin/article/2024/1715086662_file_1.pdf (дата обращения 11.07.2024).
5. ADNOC, ADNOC Wins Industry Technology Award for its Panorama Digital Command Center [Electronic resource]. – URL: <https://adnoc.ae/news-and-media/press-releases/2021/adnoc-wins-industry-technology-award-for-its-panorama-digital-command-center> (дата обращения 11.07.2024).
6. Fernandes J. V. Robot citizenship and gender (in) equality: the case of Sophia the robot in Saudi Arabia // Janus. Net. – 2022. – Vol. 12, №. 2-Thematic dossier-The Middle East. Local dynamics, regional actors, global challenges. –URL: <https://repositorio.ual.pt/server/api/core/bitstreams/a92f2749-904e-4dd6-a88f-56acee88aace/content> (дата обращения 11.07.2024).

7. European Parliament. Artificial Intelligence Act [Electronic resource]. – URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (дата обращения 11.07.2024).
8. Livermore Michael A. Rule by rules // Computational Legal Studies: The Promise and Challenge of Data-Driven Research. – Cheltenham (UK): Edward Elgar Publishing, 2020. – P. 238–264.
9. Daston L. J. Classical Probability in the Enlightenment. – Princeton: Princeton University Press, 1988.
10. Meessen P. N. On Normative Arrows and Comparing Tax Automation Systems // Proceedings of the Nineteenth International Conference on Artificial Intelligence and Law [Electronic resource]. – 2023. – URL: <https://dl.acm.org/doi/10.1145/3594536.3595160> (дата обращения 11.07.2024).
11. Chalmers D. J. The singularity: A philosophical analysis // Science fiction and philosophy: From time travel to superintelligence. – 2016. – Feb 29.
12. Zhang H., Song, H., Li, S., Zhou, M., & Song, D. A Survey of Controllable Text Generation Using Transformer-based Pre-trained Language Models // ACM Computing Surveys. – 2023. – 56(3).
13. Klimt B., & Yang, Y. The Enron Corpus: A New Dataset for Email Classification Research // European Conference on Machine Learning. – 2004.
14. Penikis S., Releford, J., & Hakim, D. Uncovering Wrongdoing in the Enron Email Corpus // Glorin Sebastian's Lab. – 2023.
15. Bainbridge S. M. (2002). Director Primacy: The Means and Ends of Corporate Governance // Nw. UL Rev. – 2002.
16. Hanson Robotics [Electronic resource]. – URL: <https://www.hansonrobotics.com/sophia/> (дата обращения 11.07.2024).
17. CGI Russia. Круглый стол CGI Russia «Цифровизация корпоративного управления: войдет ли ИИ в совет директоров?» // [Электронный ресурс]. – URL: <https://cgi-russia.ru/events/cifrovizaciya-korporativnogo-upravleniya-vojdets-li-ii-v-sovet-direktorov/> (дата обращения 11.07.2024).
18. Dong H., Liu Y., Chu T., & Saddik A.E. (2024). Bringing Robots Home: The Rise of AI Robots in Consumer Electronics // ArXiv, abs/2403.14449.

В. А. Сайдашева,

кандидат технических наук, доцент,

Казанский инновационный университет имени В. Г. Тимирязева

НЕКОТОРЫЕ АСПЕКТЫ ЦИФРОВИЗАЦИИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ НА СТАДИИ ВОЗВРАТА ТОВАРОВ

Аннотация. Целью исследования стало изыскание возможностей оптимизации процессов на стадии возврата товаров с маркетплейсов посредством цифровых технологий. Маркетплейсы в настоящее время занимают все более значимые позиции в современной коммерческой деятельности. При этом как владельцы электронных площадок, так и предприниматели сталкиваются с рядом проблем на стадии возврата товаров. В качестве путей решения предлагаются логи-

стические подходы с использованием маркетинговых инструментов и достижений цифровой экономики.

Ключевые слова: цифровые технологии, маркетплейс, товар, потребители, возвраты, проблемы, электронная коммерция

SOME ASPEKTS DIGITALIZATION IN E-COMMERCE ON THE RETURN STAGE

Abstract. The goal of this article is to explore opportunities for optimizing return processes on marketplaces through digital technologies. Marketplaces are currently gaining increasingly significant positions in modern commercial activity. However, both marketplace owners and entrepreneurs encounter a number of challenges during the return stage. As potential solutions, the article suggests logistics approaches incorporating marketing tools and advancements in the digital economy.

Keywords: digital technologies, marketplace, product, consumers, returns, problems, e-commerce

Введение. Современные тенденции в экономике неоднозначны, однако с усилением глобализации и цифровизации часть их постепенно усугубляется в части приоритетов. К примеру, усиление санкционного пресса и вынужденная переориентация в качестве приоритетов на иные рынки сбыта, причем в электронном пространстве, тем не менее это не снижает предпринимательской активности российского бизнеса. Показатель немалый по значению, причем несколько больший по сравнению с прошлыми периодами, и с учетом позитивных тенденций ожидаем резерв для его роста. Ситуация менее оптимистична, если формировать сравнения с другими странами, например, в Китайской Народной Республике (КНР) удельный вес продаж путем электронной коммерции составляет 27,6%, а в Великобритании – 29,3% [2. С. 2–3].

Современные тенденции и вызовы в коммерческом предпринимательстве свидетельствуют о том, что в условиях цифровизации экономики и социальной, а также бытовой сфере потребителей все больше потребностей в товарах и услугах удовлетворяются посредством электронной коммерции, которая, однако, как и другие виды деятельности, имеет затратную составляющую, а значит подлежит оптимизации в части рационализации как логистических, так и транзакционных издержек. Последний тип издержек формируется и имеет тенденцию к увеличению в связи с тем, что количество покупок увеличилось, а средний чек уменьшился, поэтому затраты на промежуточные действия по доле растут. Как свидетельствует опыт коммерческой деятельности, особенно на маркетплейсах, возвраты приносят немало проблем владельцам бизнеса и формируют нежелательные траты, порой существенно увеличивающие издержки обращения. Результаты исследований, проведенных специалистами ассоциации реверсивной логистики, выявили, что, финансовые траты на управление возвратными потоками составляют приблизительно 10% от общих затрат, формирующихся в современных цепях поставок.

В целях выявления резервов оптимизации структуры возвратных материальных потоков сделаем анализ возвратов с маркетплейсов по различным параметрам. Для этого классифицируем «возвращателей» по группам, что довольно

проблематично, поскольку покупатели существенным образом различаются между собой по многим признакам, в частности: по мотивам покупки, по финансовым возможностям, по социальному статусу, по значимости товара и готовности заплатить за него назначенную цену, по срочности приобретения, по культурным аспектам, по степени приверженности онлайн-торговле и ряду других. Тем не менее обработка статистических данных предоставляет предпринимателям не только информацию к размышлению, но и дает основание для формирования рекомендаций по сокращению затрат на возвратные товарные потоки от покупателей:

- первая группа – «серийные возвращатели»;
- вторая группа – «ритейл-возвращатели» (сфера B-2-B);
- третья группа – «несистемные возвращатели»;
- четвертая группа – это «умышленные возвращатели» (так называемые потребительские эстремисты);
- пятая группа – «посреднические оптовые возвращатели»;
- шестая группа – «возвраты по невыкупленным заказам».

«Серийные возвращатели» – это категория покупателей, которые после покупки пользуются товаром, а затем возвращают его под разными предлогами (например, «не подошел фасон»). Согласно статистическим данным, чаще всего такие возвраты проявляются в сегменте товаров «верхняя одежда», хотя в эту группу можно включить еще ряд товаров, которые обычно требуют предпродажного сервиса (примерка, консультация специалиста, показ товара в действии и т. д.).

В источниках, особенно зарубежных, часто ставится знак равенства между первыми и вторыми. Однако в данном контексте подразумеваются возвраты от магазинов, например, после приемки закупленных у поставщика товаров не только по количеству, но и по качеству.

«Несистемные возвращатели» – это покупатели, которые либо нечасто пользуются услугами маркетплейсов, либо для них именно каждый возврат при неудовлетворенном спросе не обязателен.

«Умышленные возвращатели» – это обычно сегмент покупателей, сделавших покупку способом эквайринга, и которые изначально имели цель получить кэш-бек за покупку. Это, по существу, не справедливый способ возвратов, однако некоторые коммерческие компании, имея таких покупателей в базе в качестве постоянных и довольно выгодных, мирятся с такой ситуацией («Лемана Про»). «Посреднические оптовые возвращатели» обычно формируются при неисполнении условий договора поставки в сфере B2B на уровне посреднических структур. В этой категории возвращателей во главу угла ставятся юридические основания возвратов и судебного разрешения споров.

«Возвраты по невыкупленным заказам» с маркетплейсов обычно касаются товаров эмоционального спроса, например одежды, обуви, аксессуаров, косметических товаров.

В целом это серьезная проблема современной коммерческой деятельности на электронных площадках и желательно добиваться ужесточения условий по отказам от покупок. По данным интернет-компания «inSales» возврат единицы товара обходится в 50 рублей, обратная логистика стоит от 38 до 1200 рублей за

единицу, а «последняя миля» – от 20 до 250 рублей за товар [3]. На российском рынке приняли решение к запрету возвратов ряда товаров, приобретенных на электронных площадках (уже действует запрет на возвраты контактных линз). В торгово-промышленной палате РФ предложен для введения в действие перечень товаров, не подлежащих возврату. Вместе с тем следует учесть весьма интересные статистические данные проведенных маркетинговых исследований. В результате анкетирования репрезентативной выборки покупателей маркетплейсов выявлено, что «92% из них заявляют, что будут покупать снова, если процесс возврата продукта будет легким» [4. С. 11–12]. Кроме того, никто не отменял сервисную составляющую на конкурентном рынке в борьбе за покупателя и действующий федеральный закон «О защите прав потребителей». Следует ожидать, что отказы и возвраты, а значит и реверсивные материальные потоки будут формироваться, в связи с этим планирование, управление и контроль за этими потоками в перспективе будут актуальны. Поэтому предпринимателям в сегменте e-commerce придется и в будущем решать такую проблему, в том числе используя логистические принципы.

Отметим, что на количество и структуру возвратов отчасти влияют маркетинговые промо-инструменты, заложенные в элементе «promotion» базовой концепции маркетинга 4P. Как результат нейролингвистического программирования потребителя – тенденция к формированию «виртуального шопполизма» [5]. Эта группа потребителей по результатам проведенных маркетинговых исследований как импульсивно быстро приобретает товары, также довольно быстро и часто отказывается от сделанных покупок.

С одной стороны, коммерческая деятельность на электронных площадках – это действенный инструмент увеличения объема продаж, а значит и прибыли, с другой – одна из причин увеличения количества возвратов от конечных потребителей, клиентов маркетплейсов. На стадии возвратов в логистической деятельности сформированы варианты отправки и последующих действий в отношении обратных потоков, что в случае предварительного анализа и использования дает основание к оптимизации транзакционных издержек, минимизируя потери.

Заключение. Резюмируя вышеизложенное по выявленным проблемам, отметим следующее:

1. Возвраты после покупок на маркетплейсах носят регулярно-постоянный характер, формируя реверсивные материальные потоки.
2. Для разработки результативных мероприятий по снижению финансовых и временных потерь от возвратов на маркетплейсах следует изучить статистику отказов по основным причинам и структуру возвратов.
3. Российское законодательство должным образом не регулирует интернет-торговлю на маркетплейсах, поэтому основные проблемы и последствия «ложатся на плечи» предпринимателей.
4. В целях уменьшения количества возвратов следует корректно заполнять карточки товаров, используя современное программное обеспечение и минимизируя негативный человеческий фактор.

5. Работа с возвратами на маркетплейсах может стать более эффективной в случае привлечения специалистов с проведением независимой товарной экспертизы (например, на аутсорсинге).

Кроме того, продавцам сегмента e-commerce следует постоянно декларировать покупателям информацию о том, чтобы полученный с маркетплейса товар был сразу тщательно осмотрен ими после получения.

Список литературы

1. Ассоциация компаний интернет торговли. Аналитика [Электронный ресурс]. – URL: <https://akit.ru/analytics/analyt-data> (дата обращения: 01.09.2024).
2. Черешнев М. Развитие внешней торговли и международных экономических отношений [Электронный ресурс]. – URL: <https://globalmsk.ru/person/id/10801> (дата обращения: 01.09.2024).
3. Правила работы с возвратами на маркетплейсах: условия торговых платформ и советы по снижению показателя [Электронный ресурс]. – URL: <https://www.insales.ru/blogs/university/pravila-raboty-s-vozvratami> (дата обращения: 01.09.2024).
4. В России растет доля экспортеров. Материалы внешнеэкономического форума. 29 мая 2024 года. [Электронный ресурс]. – URL: <https://iz.ru/1701661/mariia-stroiteleva/mal-da-prodal-chislo-nebolshikh-kompanii-eksporterov-vyroslo-v-15-raza> (дата обращения: 01.09.2024).
5. Сарычева С. Как написать политику возврата товаров [Электронный ресурс]. – URL: <https://priceva.ru/blog/article/kak-napisat-politiku-vozvrata-tovarov> (дата обращения: 01.09.2024).
6. Матушевич С. Почему происходят возвраты в e-commerce и как сделать так, чтобы их было меньше [Электронный ресурс]. – URL: <https://habr.com/ru/articles/660343/> (дата обращения: 01.09.2024).

Н. С. Селиверстова,

кандидат экономических наук, доцент,

Казанский (Приволжский) федеральный университет,

О. В. Григорьева,

кандидат биологических наук, доцент,

Казанский инновационный университет имени В. Г. Тимирязова

СУЩЕСТВЕННЫЕ И ЧАСТНЫЕ ПРИЗНАКИ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ КАК КОНВЕРГЕНТНОГО ФАКТОРА СТРУКТУРНЫХ СДВИГОВ

Аннотация. Цель статьи в описании выявленных частных и существенных признаков цифровизации как фактора структурных сдвигов. Выделены и классифицированы признаки цифровизации экономики как конвергентного фактора структурных сдвигов: существенные признаки (сокращение времени на осуществление операций, рост открытости и прозрачности деятельности) и частные признаки (техноориентированность традиционных предприятий, по-

явление и развитие платформенных бизнес-моделей, коммуникации и ведение предпринимательской деятельности посредством ИКТ).

Ключевые слова: цифровизация, экономическое развитие, структурный сдвиг, существенные признаки, частные признаки, устойчивое развитие, промышленность

ESSENTIAL AND PARTICULAR FEATURES OF DIGITALIZATION OF THE ECONOMY AS A CONVERGENT FACTOR OF STRUCTURAL SHIFTS

Abstract. The purpose of the article is to describe the identified private and essential features of digitalization as a factor of structural shifts. The features of digitalization of the economy as a convergent factor of structural shifts are identified and classified: essential features (reduction in the time for carrying out operations, increased openness and transparency of activities) and private features (technological orientation of traditional enterprises, the emergence and development of platform business models, communications and business activities through ICT).

Keywords: digitalization, economic development, structural shift, essential features, particular features, sustainable development, industry

Введение. Структурные изменения в социально-экономических системах могут носить разный характер – происходят скачкообразно, или идут непрерывно; в любом случае их динамический анализ является популярным подходом к исследованию современных экономических феноменов [4; 5]. Структурный сдвиг в экономике представляет собой значимое качественное и количественное изменение определенной социально-экономической системы, которые вызывают изменение паттернов поведения хозяйствующих субъектов [1; 3].

Однако несмотря на имеющиеся теоретические наработки о сущности структурных сдвигов и типологии, остается много вопросов практической применимости этих теорий в практике управления предприятием, а также вопросы объяснения происходящих структурных преобразований в экономике и управления ими в условиях быстрой смены технологий и широкой доступности информации и знаний.

Основная часть. Цифровые технологии становятся ядром новой системы коммуникаций, производства, обмена и распределения благ между экономическими агентами, основой развития цифровой экономики. Цифровые технологии обеспечивают выстраивание процессов работы с данными, рост качества данных. И в этих условиях цифровизация является, на наш взгляд, базовым фактором, создающим основу для устойчивого развития промышленных предприятий в широком смысле этого слова. Почему это так?

Существенными признаками цифровизации экономики являются:

1) сокращение времени на осуществление операций – четкое, конкретное представление об используемых факторах производства в каждом отдельном моменте времени;

2) рост прозрачности операций – сокрытие информации или значений тех или иных показателей затруднено в связи с автоматической фиксацией событий в информационных системах и сервисах или датчиками.

Под существенными признаками понимаются признаки, внутренне присущие природе явления, они свойственные и целому, и его отдельным частям и являются основой свойства фрактальности экономических систем – когда часть целого несет в себе свойства всего целого. Частные признаки не являются определяющими природу целого, а появляются как влияние на внешние явления (эти признаки присущи явлению в конкретный период социально-экономического развития в нашем случае, но не являются внутренне ему присущими). Это важно для понимания как именно происходит конвергенция структурных сдвигов при воздействии рассматриваемого фактора на целевой объект.

Во-первых, цифровизация дает более четкое представление об используемых ресурсах – затратные, объемные и другие показатели. Благодаря датчикам на оборудовании или в помещении, панелям ввода данных на рабочих местах (АРМ, автоматизированное рабочее место), учетным системам и сервисам (например, конкретные продукты 1С ERP, 1С УПП и др.), средствам мониторинга (например, KICS for Networks, MLAD для промышленных сетей АСУТП от вендора Kaspersky) мы имеем детальное представление о производственных процессах и о том, как эти события влияют на финансовые показатели предприятия. Все вместе это создает инфраструктурные условия для поиска путей оптимального, а значит более устойчивого, развития каждого отдельного предприятия. Широкое использование учетных систем создает возможность для:

1. Проведения анализа, расчетов и выбора оптимального экономического способа производства с точки зрения затрат ресурсов, в том числе материальных ресурсов и энергии;
2. Оценки потенциальных эффектов от внесения изменений в производственные и вспомогательные процессы, подготовки аргументов при защите инвестиционных проектов.

Цифровизация предполагает более быстрый и зачастую более дешевый доступ к данным, с помощью которых можно планировать, имитировать, моделировать деятельность производственных объектов (цифровые двойники (англ. Digital twins), модели предиктивной аналитики, системы бизнес-анализа (Business Intelligence) и другие). Это позволяет менять бизнес-модели, логику и практику принятия управленческих решений, менять подход к управлению предприятием в целом.

Во-вторых, сокрытие информации о фактических значениях показателей, работе оборудования становится затруднено в связи с автоматической фиксацией значений и передачей этих данных, а также их дальнейшей обработки и визуализации агрегированных результатов.

Частными признаками цифровизации как конвергентного фактора структурных сдвигов, на наш взгляд, могут служить:

- 1) *техноориентированность традиционных предприятий*. Это проявляется в том, что многие традиционные компании перестраивают стратегию развития в сторону превращения в технологические и/или экосистемные компании. Например, Сбербанк принял в 2017 году стратегию превращения в технологическую компанию. Компания и в настоящее время продолжает развивать экосистему, где банковский бизнес является одним из направлений деятельности. МТС, OZON и Wildberries также развивают собственные цифровые экосистемы.

2) *появление и развитие платформенных бизнес-моделей*. По данным ИС-ИЭЗ НИУ ВШЭ, «распространение цифровых платформ в регионах преобразует экономический ландшафт страны. В 2021 г. в целом по России цифровые платформы задействовали 14,7% предприятий» [2].

3) *коммуникации и ведение предпринимательской деятельности посредством ИКТ*. Так, например, число обращений к цифровым ресурсам в России, по данным Росстата (ФСГС) существенно увеличилось в 2021 и 2022 годах.

Таким образом, схема взаимовлияния цифровизации и устойчивого развития в контексте структурных сдвигов приведена на рисунке 1.

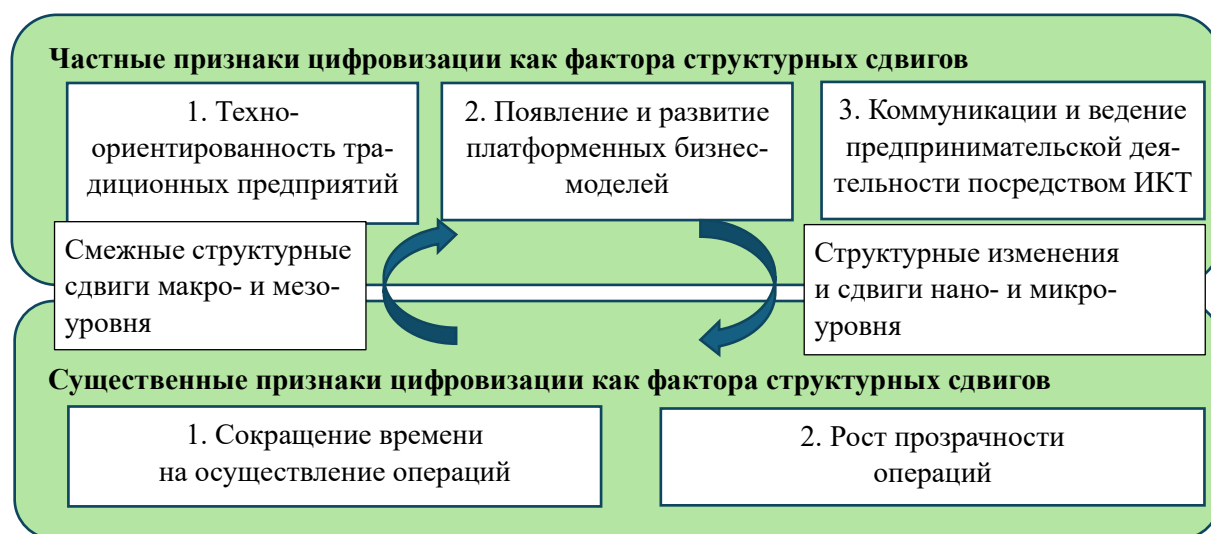


Рис. 1. Схема взаимовлияния частных и существенных признаков цифровизации

Заключение. В заключении хотелось бы отметить, что показателем структурного сдвига являются не только сами статистические данные по натуральным показателям деятельности компаний, но и институциональные изменения. Так, Росстат начал собирать информацию о платформенной занятости в рамках выборочного обследования рабочей силы (ОРС) с 2022 г. Это является примером институциональных изменений в результате развития новых бизнес-моделей – что отражает поведенческий компонент структурного сдвига – перестройку моделей взаимодействия экономических субъектов.

Все эти изменения подтверждаются *изменением структуры затрат предприятий*: ростом доли затрат на связь, ИТ-услуги, ИТ-товары. И появление новых рынков и рыночных ниш – развитие рынка системной интеграции и др.

Список литературы

1. Красильников О. Ю. Теоретико-методологические основы исследования структурных сдвигов в современной российской экономике: диссертация на соискание ученой степени доктора экономических наук: 08.00.01 – Саратов, 2001. – 312 с.

2. Орлова В., Фролов М., Мартынов Д. Цифровые платформы повышают связность регионов // ИСИЭЗ НИУ ВШЭ [Электронный ресурс]. – URL: <https://issek.hse.ru/news/799503676.html> (дата обращения: 16.05.2023).

3. Селиверстова Н. С. Систематизация методологических подходов к структурному анализу экономики, идентификации структурных изменений и сдвигов // Вестник Южно-Уральского государственного университета. Серия: Экономика и менеджмент. – 2023. – Т. 17, № 3. – С. 122–131.

4. Селиверстова Н. С., Шкутько О. Н., Григорьева О. В. Структурные изменения средне технологичных отраслей экономики в условиях цифровой трансформации промышленности // Russian Journal of Economics and Law. – 2023. – Т. 17. – № 3. – С. 532–547.

5. Huang J., Zhang H., Peng W., Hu C. Impact of energy technology and structural change on energy demand in China // Science of the Total Environment. – 2021. – №760. – С. 143–345.

Ю. М. Сметанин,

кандидат физико-математических наук, доцент,

Удмуртский государственный университет,

В. М. Сметанина,

студент,

Московский государственный технический университет

имени Н. Э. Баумана,

Г. А. Бусоргин

студент,

Московский государственный юридический университет

имени О. Е. Кутафина (МГЮА)

ВЕРИФИКАЦИЯ ВЕРСИЙ РАССЛЕДОВАНИЯ НА ОСНОВЕ КОМПЬЮТЕРНОЙ ЛОГИКО-СЕМАНТИЧЕСКОЙ МОДЕЛИ

Аннотация. В работе [4] обоснована возможность формализации следственной ситуации в цифровой логико-семантической модели для текущего состояния информационной базы расследования. Модель представлена с помощью формул на основе атомарных высказываний универсальной силлогистики L_{S_2} . Атомарные высказывания и конъюнктивные формулы, составленные из них, имеют семантические значения в виде множества из неотрицательных целых чисел либо пустого множества. От множества известных силлогистик универсальная силлогистика отличается возможностью выражать посредством конъюнктивной формулы односмысловые высказывания.

С помощью компьютерной модели находится семантическое значение формулы L_{S_2} , описывающей версию, и проверяется, является ли она логическим следствием из информации, доступной на данном этапе расследования. Также программа позволяет наглядно изображать логические связи в форме дискретной диаграммы Венна. Идейно данный подход восходит к работам П. С. Порецкого.

Рассматриваемая цифровая модель с успехом может быть использована для формирования и отладки инструкций, регламентирующих деятельность.

Ключевые слова: цифровизация логико-семантических моделей, силлогистика, приложения логики, принятие решений, верификация логического следования.

CONSTRUCTION AND VERIFICATION OF VERSIONS IN THE INVESTIGATION PROCESS BASED ON A COMPUTER LOGICAL-SEMANTIC MODEL

Abstract. The paper [4] substantiates the possibility of formalizing the investigative situation in a digital logical – semantic model for the current state of the information base of the investigation. The model is presented using formulas based on atomic statements of universal syllogistics.

Atomic statements and conjunctive formulas made up of them have semantic meanings in the form of a set of non-negative integers or an empty set. Universal syllogistics differs from many well-known syllogistics in the ability to express single-meaning statements by means of a conjunctive formula. The computer program calculates the semantic meaning of the universal syllogistic formula describing the version, and allows you to check whether it is a logical consequence of the information available at this stage of the investigation. The program also allows you to visually depict logical connections in the form of a discrete Venn diagram. Ideologically, this approach goes back to the works of P. S. Poretsky.

Keywords: process of investigating criminal cases, digitalization of logical - semantic models, syllogistics, applications of logic, decision-making, verification of logical consequence.

Введение. Субъект расследования имеет дело с отражением на материальных носителях различной природы – материальной обстановке, памяти участников и очевидцев преступления.

Процесс расследования – познавательная деятельность, в которой выявляются связи между фактами и обстоятельствами субъектами и объектами преступления. Он восходит от знания о настоящем – к знанию о прошлом. Вехами, отмечающими процесс расследования, служат следственные ситуации и версии, выдвигаемые на основании текущей информационной базы и логико-семантической модели (следственной ситуации).

Основная часть. Рассмотрим, в каком соотношении находится булева логика высказываний и универсальная силлогистика.

1. Сопоставим модельным множествам X_i булевы переменные x_i так что x_i являются характеристическими функциями для X_i , то есть

$$\forall e \in U \left(x_i(e) = \begin{cases} 1, e \in X_i \\ 0, e \notin X_i \end{cases}, i = \overline{1, n} \right).$$

2. Любая формула булевой логики $F(\mathcal{X}_n)$ от n переменных x_i может быть рассмотрена как логическое уравнение (равенство) $F(\mathcal{X}_n) = 1$. Левая часть этого

равенства может быть представлена любой другой формулой, равносильной $F(\mathcal{X}_n^0)$, в том числе совершенной дизъюнктивной нормальной формой.

3. Заменяем в равенстве $F(\mathcal{X}_n^0) = 1$ характеристические функции модельных множеств x_i на соответствующие им модельные множества X_i , а единицу на универсум U . Между равенствами $F(\mathcal{X}_n^0) = 1$ и $F(\mathcal{X}_n^0) = U$ существует соотношение изоморфизма.

4. Чтобы перевести равенства формулы логики высказываний в равенства $F(\mathcal{X}_n^0) = 1$ формулы булевой логики используется равносильные формулы $x \oplus y \equiv (x \cdot y' + x' \cdot y)$; $x \Rightarrow y \equiv x' + y$; $x \Leftrightarrow y \equiv (x' + y) \cdot (x + y')$.

5. Чтобы соотнести атомарные высказывания универсальной силлогистики с равенствами $F(\mathcal{X}_n^0) = U$, используем равносильности, установленные еще во времена Венна.

$$A(X, Y) \equiv X \cdot Y' = \emptyset \equiv X' + Y = U; Eq(X, Y) \equiv X \cdot Y' + X' \cdot Y = \emptyset \equiv (X' + Y) \cdot (X + Y') = U$$

Например, $A(X, Y) \cdot Eq(Y, Z) \equiv (X' + Y) \cdot (Y' + Z) \cdot (Y + Z') = U$. Отсюда следует, что $U = (\{0..3\} + \{2, 3, 6, 7\}) \cdot (\{0, 1, 4, 5\} + \{1, 3, 5, 7\}) \cdot (\{2, 3, 6, 7\} + \{0, 2, 4, 6\}) = \{0, 3, 7\}$. Этому универсуму сопоставляется диаграмма, изображенная на рис. 2.

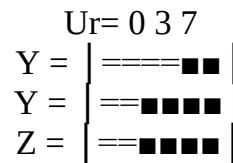


Рис. 2. Диаграмма для формулы $A(X, Y) \cdot Eq(Y, Z)$

Таким образом, вырожденная логика высказываний с семантическими значениями ложь (0) и истина (1), в которой наличествует парадокс материальной импликации, может быть заменена универсальной силлогистикой, основанной на алгебраической системе.

Рассмотрим пример перехода от конъюнктивной формулы логики высказываний к конъюнктивной формуле универсальной силлогистики.

$$[a' \cdot c' \Rightarrow e \cdot (b + d) \cdot (b \cdot d)]' \cdot [a \cdot d \cdot e' \Rightarrow (b \cdot c + b' \cdot c')] \cdot$$

$$[(a \cdot (b + e) \Rightarrow (c \cdot d' + c' \cdot d)) \cdot ((c \cdot d' + c' \cdot d) \Rightarrow a \cdot (b + e))] = 1$$

Заменяем подформулы с импликацией равносильными

$$[(a' \cdot c')' + e \cdot (b + d) \cdot (b \cdot d)]' \cdot [(a \cdot d \cdot e')' + (b \cdot c + b' \cdot c')] \cdot$$

$$[(a \cdot (b + e))' + (c \cdot d' + c' \cdot d)) \cdot ((c \cdot d' + c' \cdot d)' + a \cdot (b + e))] = 1$$

Далее заменяем булевы переменные модельными множествами и получаем равенство являющееся КППФ универсальной силлогистики.

$$[(A' \cdot C')' + E \cdot (B + D) \cdot (B \cdot D)]' \cdot [(A \cdot D \cdot E')' + (B \cdot C + B' \cdot C')] \cdot \quad (4)$$

$$[(A \cdot (B + E))' + (C \cdot D' + C' \cdot D)) \cdot ((C \cdot D' + C' \cdot D)' + A \cdot (B + E))] = U$$

Процесс доказывания (формирования версионного умозаключения) в каждой следственной ситуации реализуется итерационной процедурой состоящей как минимум из пяти этапов:

- 1) количественное накопление и структуризация фактических данных;
- 2) совокупная логическая оценки этих данных и формирования версий;
- 3) верификация версий с фиксацией возможных и необходимых для версии заключений;
- 4) выявление неполноты фактической базы для каждой из перспективных версий и планирование следственных действий по ее пополнению;
- 5) уточнение (корректировка) предыдущей следственной ситуации и построение следующей следственной ситуации, исходя из реалий процесса расследования.

«Основные функции версий – объяснительная, установительная, проверочная» [1. С. 79].

В литературе [1] выявлены три различные формы связи между ними: **необходимой, сопутствующей** (возможной), а также наиболее сильной и редкой – **необходимой и достаточной**.

Возможная форма связи иллюстрируется примером 1.

Пример 1. Пусть имеет место система из двух посылок, выраженных многозначными категорическими суждениями Аристотеля. Все M есть P и некоторые P есть S . Логично предположить, что некоторые из M есть S . В нотации категорических суждений Аристотеля

$$AMP \cdot IPS \not\models IMS$$

Многозначность категорических суждений не позволяет уточнить при каких сочетаниях смысловых значений посылок эта возможность реализуется. Универсальная силлогистика позволяет это сделать. Запишем категорические утверждения посылок через атомарные высказывания силлогистики L_{S_2} смотри ниже. Наглядно случаи изображены на рис. 5.

$$AMP \cdot IPS \equiv [A(M, S) + Eq((M, S))] \cdot [A(P, S) + Eq(P', S) + A(S', P') + A(S, P) + IO(S, P)] \equiv$$

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) & A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) & A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) & A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) & A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) & A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) & A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) & A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) & A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) & A(M, P) \cdot A(P, S) \cdot A(M, P) \cdot Eq(P', S) \cdot A(M, P) \cdot A(S', P') \cdot A(M, P) \cdot A(S, P) \cdot A(M, P) \cdot IO(S, P) \end{array}$$

В случаях 1, 4, 5, 10 никакой логической связи между модельными множествами, отражающими фактологию, нет. В случаях 2, 3, 8 принадлежность множеству M влечет за собой принадлежность множеству S . Случаи 6, 7, 9 можно считать с рисунка. Таким образом, разбор случаев позволяет построить таблицу решений для обоснованных логических выводов (табл. 1). Эта таблица является таблицей решений систематизирующей результаты разбора всех десяти случаев.

Таблица 1

Таблица решений для разбираемого примера

Номер случая	1, 4, 5, 10	2, 3, 8	6	7	9
Следствие	$IO(M, S)$	$A(M, S)$	$A(M', S)$	$EQ(M, S)$	$A(S, M)$

$$1) A(M,P) \cdot A(P^{\wedge},S) \not\models IO(M,S)$$

$$Ur = 1\ 2\ 3\ 6\ 7$$

$$X1 = |=====■ ■ ■ ■ | M$$

$$X2 = |==■ ■ ■ ■ ■ ■ ■ ■ | P$$

$$X3 = |■ ■ ==■ ■ ==■ ■ | S$$

$$6) EQ(M,P) \cdot A(P^{\wedge},S) \not\models A(M^{\wedge},S)$$

$$Ur = 1\ 6\ 7$$

$$X1 = |==■ ■ ■ ■ | M$$

$$X2 = |==■ ■ ■ ■ | P$$

$$X3 = |■ ■ ==■ ■ | S$$

$$2) A(M,P) \cdot EQ(P,S) \not\models A(M,S)$$

$$Ur = 0\ 3\ 7$$

$$X1 = |====■ ■ | M$$

$$X2 = |==■ ■ ■ ■ | P$$

$$X3 = |==■ ■ ■ ■ | S$$

$$7) EQ(M,P) \cdot EQ(P,S) \not\models Eq(M,S)$$

$$Ur = 0\ 7$$

$$X1 = |==■ ■ | M$$

$$X2 = |==■ ■ | P$$

$$X3 = |==■ ■ | S$$

$$3) A(M,P) \cdot A(S^{\wedge},P^{\wedge}) \not\models A(M,S)$$

$$Ur = 0\ 1\ 3\ 7$$

$$X1 = |====■ ■ | M$$

$$X2 = |====■ ■ ■ ■ | P$$

$$X3 = |==■ ■ ■ ■ ■ ■ | S$$

$$8) EQ(M,P) \cdot A(S^{\wedge},P^{\wedge}) \not\models A(M,S)$$

$$Ur = 0\ 1\ 7$$

$$X1 = |====■ ■ | M$$

$$X2 = |====■ ■ | P$$

$$X3 = |==■ ■ ■ ■ | S$$

$$4) A(M,P) \cdot A(S,P) \not\models IO(M,S)$$

$$Ur = 0\ 2\ 3\ 6\ 7$$

$$X1 = |====■ ■ ■ ■ | M$$

$$X2 = |==■ ■ ■ ■ ■ ■ ■ ■ | P$$

$$X3 = |====■ ■ ==■ ■ | S$$

$$9) EQ(M,P) \cdot A(S,P) \not\models A(M^{\wedge},S^{\wedge})$$

$$Ur = 0\ 6\ 7$$

$$X1 = |==■ ■ ■ ■ | M$$

$$X2 = |==■ ■ ■ ■ | P$$

$$X3 = |====■ ■ | S$$

$$5) A(M,P) \cdot IO(P,S) \not\models IO(M,S)$$

$$Ur = 0\ 1\ 2\ 3\ 6\ 7$$

$$X1 = |====■ ■ ■ ■ | M$$

$$X2 = |====■ ■ ■ ■ ■ ■ ■ ■ | P$$

$$X3 = |==■ ■ ==■ ■ ==■ ■ | S$$

$$10) EQ(M,P) \cdot IO(P,S) \not\models IO(M,S)$$

$$Ur = 0\ 1\ 6\ 7$$

$$X1 = |====■ ■ ■ ■ | M$$

$$X2 = |====■ ■ ■ ■ | P$$

$$X3 = |==■ ■ ==■ ■ | S$$

Рис. 5. Иллюстрация разбора несовместных случаев возможностного вывода

Процесс проверки должен завершиться одним из трех вариантов:

1. Неподтверждение следствий, выведенных из проверяемой версии, т. е. необнаружение предполагаемых фактов. Это означает лишь неполучение по различным причинам ожидаемой информации, что не опровергает возможностную связь. Дело в том, что неподтверждение логических следствий может быть вызвано не только объективными причинами, но и неэффективным проведением процессуальных, оперативно-розыскных или экспертных действий. Это подтверждается многочисленными случаями из практики.

2. Опровержение логических следствий [1].

3. Полученное следствие находится в отношении необходимости и достаточности по отношению к версии. Это указывает на ее справедливость.

Интерпретируем пример 1 следующим образом.

M – множество или один элемент универсума обладающий свойством быть убийцей в данном преступлении.

P – множество людей, которые были в одной компании во время убийства.

Установлено, что убийца (убийцы) принадлежат множеству P – АМР.

S – множество материальных объектов – носители следов преступления.

Возможно, на теле или одежде членов компании остались следы преступления (IPS). Более точно IPS означает, что некоторые лица (лицо) из множества P являются(ются) носителем следов либо имеет отношение к вещдокам обнаруженным на месте убийства. В компании выявлены две личности.

$M = \{П1, П2\}$ П1 и П2, имеющие криминальное прошлое были в одной компании с убитым. Они попали под подозрение (возможно, что убийство совершили П1 или П2).

Версия. Возможно, П1 или П2 – убийцы IMS. Связь версии с фактологией имеет логическую структуру примера 1 – $(AMP \cdot IPS \models IMS)$.

Разбор случаев, изображенных на рис. 5 и в табл. 1, сразу предлагает обратить внимание на случаи 2, 3, 8, из которых с необходимостью следует, что П1 или П2 убивали. Случай 2 отвергнут, так как не все члены компании на основании установленных фактов, являются носителями следов преступления либо имеют отношение к другим носителям следов. Случаи 3 и 8 указывают на то, что подозреваемые являются носителями следов, либо имеют отношение к следам, это увеличивает возможность справедливости данной версии. Случай 6 опровергает данную версию на основе установленных на данном этапе фактологической базе, если компания состояла не только из П1, П2, и убитого.

Случаи 1, 4, 5 не опровергают версию, для того чтобы его свести к случаю 3 необходимо доказать на существующей базе фактов, что подозреваемые имеют отношение к следам преступления либо являются их носителями. Если фактическая база не позволяет это сделать, то, придерживаясь данной версии, необходимо производить новые поисковые мероприятия. Случай 9 указывает, что П1 и П2, имеющие криминальное прошлое, были в одной компании с убитым и в компании, кроме убитого, присутствовали только они, и что оба они являются носителями следов, что указывает на их участие в преступлении.

Исходные посылки выглядят как

$$P_1 : A = U; P_2 : A' \cdot C' \subset E \cdot (B + D) \cdot (B \cdot D); P_3 : A \cdot D \cdot E' \subset (B \cdot C + B' \cdot C');$$

$$P_4 : A \cdot (B + E) = C \cdot D' + C' \cdot D;$$

В универсальной силлогистике КППФ, выражающая эти логические отношения имеет вид (8)

$$A \cdot (A[A' \cdot C', E \cdot (B + D) \cdot (B \cdot D)] \cdot A[A \cdot D \cdot E', (B \cdot C + B' \cdot C')]) \cdot Eq[A \cdot (B + E), C \cdot D' + C' \cdot D] \quad (8)$$

Модельные множества (признаки) находятся в следующих логических отношениях описываемых формулой (8), пятиарное логическое отношение (семантическое значение формулы) изображено на рис. 5. Пусть семантика (объемное содержание отношения) и формула (логическое содержание) отражают сложившуюся на данный момент фактическую базу, исходя из которой выдвинута гипотеза о том, что преступниками могут быть только субъекты, из модельного множества A .

Список литературы

1. Криминалистика: учебник для вузов: в 3 ч. Ч.1 / отв. ред. Л. Я. Драпкин. – 2-е изд., испр. и доп. – М.: Юрайт, 2022. – 246 с.
2. Кузичев А. С. Диаграммы Венна. – М.: Наука, 1968. – 253 с.
3. Сметанин Ю. М. Фронтальный алгоритм решения SAT задачи // Программные системы: теория и приложения. – 2022. – № 13. – С. 163–179.
4. Сметанин Ю. М. Сметанина В. М. О возможности цифровизации и компьютерной верификации версий в процессе расследования – Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 4. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – С. 298–306.
5. Сметанин Ю. М. Верификация логического следования в неклассической многозначной логике // Известия Института математики и информатики УдГУ. – 2017. – Т. 50. – С. 62–82.
6. Сметанин Ю. М., Сметанина В. М., Оганесян А. А. Синтез таблиц решений и следствий из системы продукций с использованием универсальной силлогистики // Академическая наука – проблемы и достижения – Academic science – problems and achievements XXXII : материалы XXXII междунар. науч.-практ. конф. (13–14 июня 2023 г., Bengaluru, India). – Bengaluru, 2023. – С. 162–180.
7. Сметанин Ю. М., Сметанина Л. П. Логические аспекты информационно-аналитической работы (как сложить мозаику) [Электронный ресурс] // Современные проблемы профессионального образования: опыт и пути решения : материалы Пятой Всерос. науч.-практ. конф. с междунар. участием, приурочен. к 90-летию Иркутск. нац. исследоват. техн. ун-та и к 45-летию Иркутск. гос. ун-та путей сообщения. – Иркутск: Изд-во ИрГУПС, 2020. – С. 517–521.
8. Smetanin Iu. Syllogistical System on the Basis of the Propositional Multi-valued Logic ypc] // 2015 International Conference "Stability and Control Processes" in Memory of V. I. Zubov (SCP) : Russia, Saint-Petersburg, October 5–9, 2015 / editors: L. A. Petrosyan, A. P. Zhabko. – Saint-Petersburg: IEEE, 2015. – P. 596–599.

А. В. Хмелев,
старший преподаватель,
Сибирский государственный университет
телекоммуникации и информатики
Д. Д. Матюнин,
ассистент, магистр,
Сибирский государственный университет
телекоммуникации и информатики
Е. В. Попова,
стажер-лаборант,
Сибирский государственный университет
телекоммуникации и информатики

ЦИФРОВЫЕ СЕРВИСЫ КАК ИНСТРУМЕНТ ДЛЯ ПОИСКА АЛЬТЕРНАТИВНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ТЕКУЩИХ РЕАЛИЯХ

Аннотация. Сегодня в отечественной экономике есть потребность в новых сервисах, так, например, нужны сервисы, позволяющие находить тот или иной программный продукт, так как большая часть сейчас используемого программного обеспечения импортная, а подобные сервисы могут быть инструментом, позволяющим оперативно находить альтернативу. В данном материале изучаются ключевые аспекты, важные для создания сайта помощника по поиску программного обеспечения в области сайтостроения и дизайна, в частности база данных как основа, и технические параметры продуктов (так как в сфере бизнеса есть определенные сложности с модернизацией технического оснащения сегодня).

Ключевые слова: цифровые технологии, сервисы помощники, альтернативные инструменты, программное обеспечение, технические критерии, совместимость

DIGITAL SERVICES AS A TOOL FOR SEARCHING FOR ALTERNATIVE SOFTWARE IN THE CURRENT REALITIES

Abstract. At the moment, there is a need for new services in the domestic economy, for example, services are needed that allow you to find a particular software product, since most of the software currently used is imported, and such services can be a tool that allows you to quickly find an alternative. This material examines the key aspects important for creating a software search assistant site in the field of website building and design, in particular the database as a basis, and the technical parameters of the products (since in the business sphere there are certain difficulties with modernizing technical equipment today).

Keywords: digital technologies, assistant services, alternative tools, software, technical criteria, compatibility

Введение. Современные реалии таковы, что сегодня многие иностранные компании перекрывают доступ к своим программным продуктам. Кто-то не про-

дает лицензии пользователям из России, кто-то, как, например «Conva», блокирует доступ к своей площадке для пользователей из РФ и размещает осуждающие объявления (с чем столкнулись студенты заочного и дистанционного обучения, ведь ранее данный ресурс был бесплатным и не требовал установки на персональный компьютер, что делало его востребованным для данных групп обучающихся и не только) [8].

Основная часть. Необходимо понимать, что программы (онлайн или с установкой на ПК) также играют большую роль в функционировании субъектов малого бизнеса (в частности, для средств массовой информации и маркетплейсов) [3; 6; 10]. Так, сейчас многие сайты делаются через конструктор сайтов Tilda [11], так как для этого не нужны познания в программировании, а услуги компаний, специализирующихся в этой области стоят существенных денежных средств, но если допустить что данный конструктор иностранный и перестанет работать, а все сайты созданные на нем будут не доступны, как и с блокировкой «Conva», появляется необходимость в альтернативе, то есть в аналоге, на базе которого можно быстро создать сайт (если графические элементы, используемые ранее сохранились) и тем самым оперативно возобновить работу. Для примера, в качестве альтернативы Tilda можно использовать Celestra [9], но, как показал опрос, среди студентов третьего курса направления «09.03.02. Информационные системы и технологии в медиаиндустрии» (СибГУТИ), о таком аналоге они не знают, хотя есть предмет, связанный с сайтостроением и созданием графических интерфейсов. Получается, чтобы оперативно решить проблему нужно или владеть огромным объемом информации, или же нужен сервис в сфере сайтостроения и дизайне, который работал бы по принципу «Сравни.ру» [7] или «Банки.ру» [1].

Для создания данного сервиса нужно учесть несколько важных моментов:

Во-первых, (а) база данных. В данной теме понимается перечень инструментов и ресурсов (нужно понимать, что речь идет о сфере сайтостроения и дизайна, и задачи можно решать, как программами, так и языками программирования).

(б) создание сайта на базе конструктора (в рамках данной задачи стоят цели по созданию работоспособного сайта на платформе конструктора, для данной задачи нужно не только знание дизайна (как для первой), но и знание программирования, так как могут возникать задачи, связанные с написанием кода), для реализации можно использовать: Tilda, Celestel, uCoz, Wix, uKit, MotoCMS, WordPress, DLE, InstantCMS;

(в) создание сайта посредством программирования (данная задача больше относится к сфере программирования, так как в рамках нее ведется создание того, что чаще всего называется исходным кодом сайта), для реализации можно использовать: Java Script, HTML, CSS, PHP, Python, SQL, Adobe Dreamweaver, Sublime Text, Visual Studio Code, WebStorm.

Получается, что есть три типа задач, и в рамках каждой задачи можно использовать 6–10 инструментов или ресурсов. Но, кроме перечня, нужен так же и функционал, выше приводился пример Tilda и Celestra, в которых есть похожие функции (многие), но есть и различия. Если при запросе сервис будет показывать

перечень функций, то это будет помогать координироваться в ракурсе вопроса – нужны еще ресурсы или какой-то один является полноценной заменой.

Во-вторых, техническое описание к программному обеспечению. Нужно понимать, что обновление технического оснащения (комплектующих ПК) на сегодня затруднено (как по причине высокой цены, так и по причине отсутствия тех или иных компонентов), это так же подтверждается тем фактом, что в 2023–2024 годах вырос спрос на ремонт компонентов в сервисных центрах. Как результат, многие субъекты бизнеса ограничены, и им может потребоваться не просто альтернативные ресурсы, но такие ресурсы, что подходили бы под их материально-техническую базу [2]. В числе таких параметров, которые необходимо отображать в таком сервисе, могут быть следующие:

Операционная система (в целом это важный аспект, так как сейчас не все продукты, в том числе отечественные, ставятся на систему Linux, также необходимо отметить, что ранее уже замечались отрицательные явления при использовании CorelDRAW на операционной системе Windows Vista);

Процессор, материнская плата и видеокарта (важные аспекты, при этом материнская плата и видеокарта еще и связаны между собой, так были выявлены случаи, что еще есть в эксплуатации «бюджетные компьютеры», то есть такие, где на материнской плате отсутствовал разъем для видеокарты, и нагрузка шла напрямую на материнскую плату, это важно, так как онлайн-программы требовательные);

Важно понимать, что, кроме вышеобозначенного, есть еще параметры, которые будут важны при выборе и эксплуатации программного продукта или ресурса. Например, технические параметры в диапазоне. Из типографской практики известно, что программа Adobe Acrobat Pro Extended во время конвертирования документа в 120–200 страниц А4 с цветными фотографиями на базе компьютера 2008–2010 годов сборки с процессором Intel Core 2 Duo может иметь длительность процесса 40–45 минут, загрузку памяти 87–92% и загрузку процессора на 100%. Это означает, что во время данного процесса нет возможности использовать другие программы, а также то, что использование ПК с еще более низкими техническими показателями может быть невозможно для реализации таких задач.

Заключение. В итоге получается, что для создания такого сервиса или сайта помощника нужно проделать большую работу как в области сбора информации и формирования базы данных, так и касательно тестирования программы на различных конфигурациях ПК для получения технической информации. При этом можно сказать, что такой сервис будет полезен как для преподавателей, так и для представителей бизнеса, кроме того, стоит отметить, что такой сервис может быть площадкой для продвижения отечественных продуктов (что может стать стимулом для разработчиков).

Список литературы

1. Банки.ру: финансовый маркетплейс [Электронный ресурс]. – URL: <https://www.banki.ru> (дата обращения: 10.09.2023).
2. Матюнин Д. Д. Сравнение стационарного программного обеспечения CorelDraw и Illustrator на двух разных конфигурациях ПК с целью определения оптимизации работы // Научное и техническое творчество молодежи: материалы Всероссийской научно-технической конференции с международным участием,

Новосибирск, 22–26 апреля 2024 года. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2024. – С. 98–101. – DOI 10.55648/NTTM-2024-1-98

3. Нуреев Р. М., Сурхаев И. Д. Цифровизация экономики: новая роль социальных сетей // Journal of Institutional Studies. – 2021. – Вып.13 (2). – С. 6–26. DOI: 10.17835/2076-6297.2021.13.2.006-026.

4. Палаш Б. В., Голубничий А. А. Базы данных в современном сайтостроении // Modern Science. – 2020. – № 2-1. – С. 380–383.

5. Попова Е. В. Анализ популярных конструкторов и инструментов для создания сайтов: особенности «Tilda» и «Celestra» // Шаг в науку: материалы II межвузовской научно-практической конференции для магистрантов, аспирантов и студентов выпускных курсов, г. Новосибирск, 07–08 декабря 2023 года. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2023. – С. 16–19

6. Попова Е. В., Хмелев А. В. Построение сайтов как важная часть развития интернет-СМИ // Экономика, менеджмент, сервис: современные проблемы и перспективы: материалы V Всероссийской научно-практической конференции, Омск, 9–10 ноября 2023 года. – Омск: Омский государственный технический университет, 2023. – С. 455–456

7. Сравни все банки, МФО и страховые в одном месте онлайн. – URL: <https://www.sravni.ru> (дата обращения: 01.09.2024).

8. Canva не работает в России с 1 июня 2022. Ищем аналоги. – URL: <https://stepvweb.ru/canva-ne-rabotaet-v-rossii> (дата обращения 1.09.2024)

9. Celestra (Целестра). URL: <https://celestra.ru> (дата обращения: 1.09.2024).

10. Nwohiri A. M., Pechnikov A. A. Application of webometrics methods for analysis and enhancement of academic site structure based on page value criterion // Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. – 2019. – Vol. 15, Iss. 3. – Pp. 337–352. <https://doi.org/10.21638/11702/spbu10.2019.304>

11. Tilda Publishing. URL: <https://tilda.cc/ru> (дата обращения: 1.09.2024).

А. В. Хмелев,
старший преподаватель,
Сибирский государственный университет
телекоммуникации и информатики
А. С. Толстиков,
магистрант,
Сибирский государственный университет
телекоммуникации и информатики

К ВОПРОСУ ВНЕДРЕНИЯ ИНТЕРАКТИВНЫХ ЭЛЕМЕНТОВ В СЛОЖНЫЕ САЙТЫ С ЦЕЛЬЮ ПОМОЩИ ПОЛЬЗОВАТЕЛЮ

Аннотация. Многие сайты имеют сложную структуру, где, чтобы найти нужную информацию, нужно с главной страницы перейти в подраздел (а их несколько), затем найти нужный раздел в нем и так далее, и не всегда пользователь

находит нужную информацию с первого раза, вследствие чего есть необходимость внедрения интерактивных элементов (нелинейного типа, что могли бы упростить поиск части информации для пользователя). В данном материале изучаются основные (ключевые) моменты при создании такого интерактивного элемента на примере разработки для Института телекоммуникации СибГУТИ.

Ключевые слова: цифровые технологии, интерактивные элементы, нелинейные, веб-структуры, поиск, удобство

TO THE QUESTION OF IMPLEMENTING INTERACTIVE ELEMENTS INTO COMPLEX SITES TO HELP THE USER

Abstract. Many sites have a complex structure, where in order to find the necessary information you need to go from the main page to a subsection (and there are several of them), then find the necessary section in it, and so on, and the user does not always find the necessary information the first time, as a result of which there is a need to implement interactive elements (non-linear type, which could simplify the search for part of the information for the user). This material studies the main (key) points in creating such an interactive element using the example of development for the Institute of Telecommunications.

Keywords: digital technologies, interactive elements, non-linear, web structures, search, convenience

Введение. Большинство сайтов сегодня это сложные много уровневые веб-конструкции с линейной системой поиска информации, это означает, что чтобы получить информацию, которая где-то в глубине, нужно с главной страницы идти в раздел, следом в подраздел и так далее, пока информация не будет найдена, при этом количество разделов и подразделов может быть огромным. Также нужно понимать, что есть документы. При этом пользователь может знать только их названия. В систему документы могут выгружаться под регистрационным номером, из-за чего пользователь также может теряться. Все вышеизложенное говорит о том, что необходимо внедрять новые технологии, что могли помогать пользователям (например, тем, кто первый раз пользуется каким-то федеральным или муниципальным сайтом). В потенциале таким инструментом можно считать нелинейные интерактивные элементы (для образовательных курсов есть примеры таких элементов, созданных в Thinglink) [1; 2].

Основная часть. Первое что нужно пояснить, что такое нелинейный – как выше было сказано, при поиске информации пользователи вынуждены идти с главной страницы в разделы и далее (так же как например листать сайт с верху вниз, или презентацию), нелинейный это означает, что с главной страницы через такой элемент можно перейти в нужный раздел, минуя промежуточные (то есть из точки «А0» в точку «Ж12», например). При этом для создания такого элемента нужно учесть ряд важных моментов, которые разберем ниже применительно для Института телекоммуникации СибГУТИ.

– Во-первых, полнота данных. Как выше упоминалось интерактивный элемент сейчас создают для курсов (то есть в нем есть точки, что отвечают за разделы курса «темы»), но такой элемент можно создать и для целой структуры

как Институт телекоммуникации. При этом нужно иметь полную информацию о количестве кафедр, количестве направлений, наличии иных структурных подразделений (например, НИЛ «научно-исследовательская лаборатория», СКБ «студенческое конструкторское бюро»). Существуют случаи, когда в одном разделе информация обновляется (например, открытие еще одного направления или магистратуры), а в другом нет, что вызывает путаницу.

– Во-вторых, структура. Структура может быть иерархическая (то есть сверху вниз от дирекции к кафедрам и далее по направлениям) (рис. 1), или географическая (когда за основу такого элемента берется стилизованное изображение вуза, и точки располагаются так, чтобы отображать место расположения дирекции и кафедр, а направления рядом с выпускающей кафедрой).

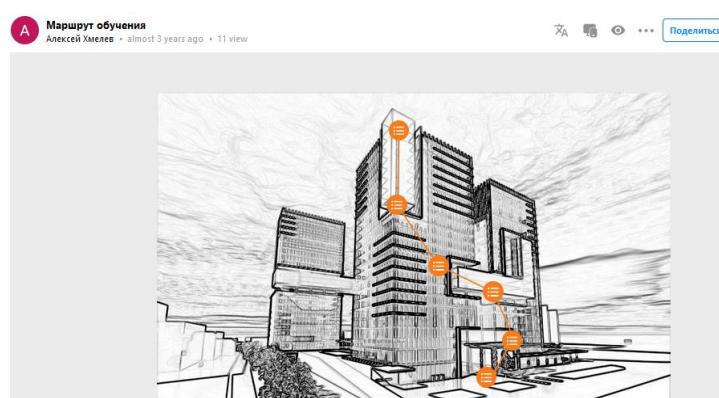


Рис. 1. Пример интерактивного элемента с иерархической системой на базе Thinglink для курса дополнительного образования

– В-третьих, графическая стилистика. В вышеобозначенной программе, на базе которой сейчас создаются интерактивные элементы, каждая точка может содержать не только краткое описание, ссылку на нужный раздел, но также тематическую картинку (рис. 2), что важно с точки зрения визуализации и сопровождения информации (так, например, точка, связанная с конструкторским направлением, может сопровождаться фото с печатью платы). Это также важно, что все фотоэлементы можно выполнить в одной цветовой стилистике, и это будет подчеркивать, что данный элемент – навигатор по Институту телекоммуникации, а аналогичные разработки для других институтов в составе СибГУТИ делать в других стилистиках.



Рис. 2. Пример наполнения точки интерактивного элемента (фотоэлемент, заголовок, текст, из существенных элементов отсутствует ссылка для перехода)

Заключение. Если подводить промежуточный итог, можно сказать, что интерактивный нелинейный элемент – это нестандартный инструмент для упрощения работы с веб-структурами, при этом нужно понимать, что, кроме создания, также важно провести исследование с целью определения, будет ли поиск информации через такой элемент быстрее, понятней, удобней.

Список литературы

1. Хмелев А. В. Использование объемных и интерактивных файлов в презентациях как способ максимизации визуальной привлекательности // Современные проблемы телекоммуникаций: материалы Международной научно-технической конференции, Новосибирск, 22–23 апреля 2021 г. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. – С. 472–475.

2. Thinglink [Electronic Resource]. – URL: <https://www.thinglink.com/edu?btnSource=logout> (дата обращения: 17.04.2024).

Э. Ш. Шаймиева,

доктор экономических наук, доцент,

Казанский инновационный университет имени В. Г. Тимирязова

Г. И. Гумерова,

доктор экономических наук, профессор,

Финансовый университет при Правительстве Российской Федерации

СОБЫТИЙНЫЙ БРЕНД КРЕАТИВНЫХ ИНДУСТРИЙ В ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ, СТАРТАП-ДВИЖЕНИИ

Аннотация. В работе исследуются вопросы взаимодействия событийных и креативных индустрий, с одной стороны, и проектной деятельности и стартап-движения – с другой. Предметом исследования является событийный бренд креативных индустрий, являющийся объектом управления в данных индустриях, исследуемых подходах (проектном управлении, стартап-движении). Информационная база исследования: базы данных Научной электронной библиотеки, цифровой платформы РОСПАТЕНТа, материалы АКАР (Ассоциации коммуникативных агентств России), Telegram-каналы событийных мероприятий, их продвижения: «Зона комфорта». Цели исследования: выявление особенностей управления событийным брендом креативных индустрий для развития проектной деятельности, стартап-движения. Методы исследования: анализ, синтез, классифицирование. Результаты исследования предназначены для развития проектной деятельности, стартап-движения «Стартап как диплом» в качестве научно-методического обеспечения (наставничества).

Ключевые слова: креативные индустрии, интеллектуальная собственность, стартапы креативных индустрий, технологическое предпринимательство, событийная индустрия, бренд событийных индустрий, проектная деятельность креативных индустрий

EVENT BRAND OF CREATIVE INDUSTRIES IN PROJECT ACTIVITIES, STARTUP MOVEMENT

Abstract. The paper examines the issues of interaction between the event and creative industries, on the one hand, and project activities and the startup movement, on the other hand. The subject of the study is the event brand of creative industries, which is the object of management in these industries, the approaches studied (project management, startup movement). Information base of the research: databases of the Scientific Electronic Library, the ROSPATENT digital platform, materials of the ACAR (Association of Communication Agencies of Russia), Telegram channels of event events, their promotion: "Comfort zone". Research objectives: to identify the features of event brand management in creative industries for the development of project activities, startup movement. Research methods: analysis, synthesis, classification. The results of the study are intended for the development of project activities within the framework of Rosmolodezh.Grants", platforms of the National Technology Initiative, the startup movement "Startup as a diploma" as scientific and methodological support (mentoring) of their activities, technological entrepreneurship in the field of event and creative industries.

Keywords: creative industries, intellectual property, startups of creative industries, technological entrepreneurship, event industry, brand of event industries, project activity of creative industries

Понятие «событийный бренд креативных индустрий» формируется на основе развития двух направлений (областей в теории и практике): креативных и событийных индустрий. Данные термины имеют определенную новизну для российского экономического пространства [5, 6]. В то время как креативные индустрии в российском экономическом пространстве опираются на нормативно-правовую базу, стремительно развивающуюся в последние пять лет, то событийные индустрии являются, в первую очередь, объектом исследования и практического применения [10, 20]. Действительно, применительно к области «креативных индустрий» относятся следующие нормативно-правовые акты, методологические документы, определяющие их развитие: Федеральный закон от 08.08.2024 № 330-ФЗ «О развитии креативных (творческих) индустрий в Российской Федерации» (далее – ФЗ «О креативных индустриях»), где представлены основные определения креативных индустрий, а именно: креативные (творческие) индустрии, креативный продукт, субъект креативной индустрии, креативный кластер [27]; «Концепции развития творческих (креативных) индустрий и механизмов осуществления их государственной поддержки в крупных и крупнейших городских агломерациях до 2030 года» (от 20 сентября 2021 г.) [9]; «Региональный стандарт развития креативных индустрий» (2023 г.) [19]. Применительно к теме настоящей работы необходимо отметить, что одним из основных понятий ФЗ «О креативных индустриях» является понятие «мер государственной поддержки в сфере креативных индустрий...», которые формируют соответствующие программы развития креативных индустрий в регионах, причем совокупность креативных индустрий представлена в «Приказе об утверждении собирательной классификационной группировки видов экономической деятельности в области

деятельности творческих (креативных) индустрий на основе Общероссийского классификатора видов экономической деятельности (ОКВЭД 2) ОК 029-2014» (2023 г.) [18]. В исследовании Ю. В. Петрашевской, где понятия «креативные индустрии» и «креативная экономика» рассматриваются в качестве синонимов, показано, что объем рынка креативных индустрий к концу 2023 года достиг «... глобальной оценки в 985 млрд дол. И вполне может составить 10% мирового ВВП к 2030 году...» [16]. В работе М. Р. Гафарова, М. Р. Сафиуллина, Л. А. Ельшина понятие «инклюзивного роста территорий» в процессе их цифровой трансформации понимается посредством «... активизации процессов встраивания хозяйствующих субъектов в систему воспроизводственных цепочек... вследствие устранения институциональных барьеров...» [4]. В качестве «институциональных барьеров» – применительно к теме настоящего исследования – здесь могут выступать процессы отсутствия регистрации прав на событийные бренды как в процессе их создания (в рамках проектной деятельности обучающихся), так и в дальнейшем жизненном цикле управления брендом креативных индустрий в виде событийного бренда сформировавшегося события (напр., фестиваля). В работе Ю. В. Беловой, Д. Ю. Ермиловой, Л. Р. Назаровой исследована «... проектная деятельность студентов по разработке дизайн-концепции для бренда в области гастро-туризма и территориального брендинга...» [2. С. 122]. В данной работе отмечается, что «... создание актуальных брендов для различных регионов России, в том числе малых и моногородов, повышает узнаваемость территории и увеличивает возможность интеграции гастрономических элементов в иные виды путешествий в данном регионе...» [2. С. 121].

В области «событийных индустрий» документами, на основе которых развиваются данные виды индустрий, по мнению авторов, являются: «Карта рынка Event-услуг» [10], согласно его разработчикам АКАР (Ассоциация коммуникативных агентств России) – «... проект инициирован комитетом event-агентств АКАР в 2023 году и проходит при поддержке РАМУ (Российская Ассоциация маркетинговых услуг) с целью развития и продвижения отечественного рынка ивентов...», «Регионы России в фокусе событийной индустрии» (2020 г.) [10, 20]. Здесь необходимо отметить, что понятие «событийной индустрии» в российском экономическом пространстве связано с понятием MICE-индустрии: М – meetings (встречи), I – incentives (инсентив, или поощрительные поездки), С – conferences (конференции), Е – events/ exhibitions (события/выставки) [11]. Согласно Н. Н. Трофимовой «... это индустрия делового взаимодействия, предполагающая корпоративные встречи, переговоры, различные обучающие программы, семинары, конференции...» [26. С. 29]. Здесь необходимо отметить объемы рынка MICE-индустрии: «... международная статистика показывает, что в 2023 г. мировой рынок MICE-индустрии составлял примерно 784 млрд долл. США...» [26. С. 29]. Согласно материалам «Карты рынка Event-услуг», выделяют следующие виды событий, формирующих рынок событийных индустрий: открытие новых проектов, выставочная деятельность, пресс-мероприятия, тимбилдинги, обучающие мероприятия, конкурсы, отраслевые и специализированные соревнования, фестивальная деятельность; конференции, форумы, саммиты; спортивные мероприятия; благотворительные и социальные мероприятия [10].

Многие из данных видов событийных индустрий являются одновременно креативными индустриями, обладающими брендом [1].

В работе Ю. А.Теслер, В. И. Теличенко исследуется парк как составляющая общественного пространства, формирующего идентичность города, отражающуюся в графическом осмыслении понятии реки как основного объекта парка Яуза [24. С. 13]. В исследовании Т. М. Вальковой, А. С.Глемейда рассматривается «гастрономический туризм», как «...новое направление. На данный вид туризма приходится около 10% от всех приобретаемых экскурсионных программ, ежегодный прирост спроса на такие поездки составляет 17% ...» [3. С. 151]. Целью работы является «...изучение теоретических аспектов развития гастрономического туризма в мире, потенциала развития данного вида туризма в АЗРФ (Арктической зоны РФ) ...» [3. С.154]. Отмечая в работе виды гастрономического туризма, участников разработки туристского продукта, а также географию проведения данных гастрофестивалей, автор подчеркивает, что «...тематические фестивали, выставки и ярмарки и др.: «День рыбака» и «День арбуза» – в Астрахани; «Праздник огурца» и «Медовуха Fest» – в Суздале; «Сыр. Пир. Мир» – в Истринском районе Московской области и пр. ... практически все подобные событийные мероприятия являются основой для формирования событийных гастрономических туров...» [3. С. 160].

Необходимо отметить, что: товарных знаков (ТЗ) «Парк Яуза», «День рыбака» и «День арбуза»; «Праздник огурца», «Медовуха Fest» на цифровой платформе Роспатента авторами не выявлено (условия поиска «строгое совпадение») [25]. Примечательно, что ТЗ, знаки обслуживания на статус «гастрономической столицы России» зарегистрированы на Муниципальное казенное учреждение Комитет по развитию туризма г. Казани (дата государственной регистрации: 20.01.2021), номер заявки: 2020702237, дата истечения срока действия исключительного права: 22.01.2030), классы Международной классификации товаров и услуг (МКТУ) 20, 35, 41 (ТЗ «Казань – гастрономическая столица России») и ООО «Кумжа» (дата подачи заявки: 19.07.2021, номер заявки: 2021745105; классы МКТУ и перечень товаров и/или услуг: 29, 30, 31, 32, 33, 40, 43) (ТЗ «Ростов-на-Дону – гастрономическая столица России») [25]. Наличие ТЗ, зарегистрированного в Роспатенте, приобретая со временем при условии эффективного управления креативный, событийный менеджмент, преобразуется в бренд соответствующей территории. Причем данный статус приобретается конкретной территорией не столько в результате соответствующего конкурса, а как результат инициативы проектной деятельности в регионе, на основе имеющихся активов в конкретном событийном, креативном направлении (в частности, гастрономическом туризме). Некоторые событийные мероприятия креативных индустрий, выбранные авторами случайным образом, на основе анализа трудов исследователей, а также упоминаемые в Telegram-канале «Зона комфорта», были проверены авторами на наличие (отсутствие) ТЗ, зарегистрированного в Роспатенте, в целях выявления особенностей в данной области управления (табл. 1) [8].

Здесь можно сделать (предварительные) выводы о том, что регистрация ТЗ как основы событийного бренда креативных индустрий не носит системный характер в российском экономическом пространстве, что характерно как для современных фестивалей, так и для событий прошлых лет (табл. 1). Данный вывод

характеризует (предположительно) современное состояние управления событийным брендом креативных индустрий, что требует дальнейшего исследования.

Таблица 1

Событийные мероприятия креативных индустрий в российском экономическом пространстве: наличие товарного знака

Наименование	Город (регион)	Дата основания	Официальный сайт	Информация о товарном знаке
Фестиваль «Креатив на Волге»	Самара	2023 г.*	https://kreativnavo.lge.ru	Правообладатель: Общество с ограниченной ответственностью Мандариновая Лиса; Дата подачи заявки: 05.03.2024
Музыкально-спортивный фестиваль «ПАРИ ФЕСТ»	Нижний Новгород	2024 г.*	https://parifest.ru	...
Всероссийский сырный фестиваль «Сыр. Пир. Мир»	Москва	2019 г.*	https://xn--h1aalkeccb4g.xn--p1ai	Правообладатель: Автономная некоммерческая организация Центр развития туризма Московской области Дата государственной регистрации: 06.12.2022 Номер заявки: 2021713081

Примечание: ... – авторами не выявлено; * – ориентировочно.

Источник: на основе [8, 13, 14, 15, 25].

В рамках развития гибких навыков обучающихся в проектной деятельности, масштабного стартап-движения, где обучающиеся разрабатывают проекты в креативных, событийных индустриях, мотивация их участников к регистрации ТЗ в Роспатенте могла бы служить достижению следующих целей: развитию навыков проектной (командной) работы над формированием, развитием объекта интеллектуальной собственности (ОИС) собственного проекта, от идеи до разработки прототипа или тестирования услуги (в случае создания нематериального продукта); развитию процессов кредитования под залог интеллектуальной собственности [12, 22, 23]. Мероприятия в рамках «мотивации» обучающихся-участников проектной деятельности, стартап-движения могут быть использованы в соответствующей программе по мерам развития креативных индустрий в регионах [19, 27]. Результаты настоящего исследования дополняют работу Ю. В. Беловой, Д. Ю. Ермиловой, Л. Р. Назаровой в части необходимости участия обучающихся в регистрации результатов их проектной деятельности в качестве ОИС [2, 17, 21, 22, 23]. Развивая идеи авторского исследования

о трудоустройстве обучающихся высшей школы, можно сделать вывод о том, что участие обучающегося в разработке ОИС с наличием свидетельства (патента) о регистрации прав в Роспатенте (или разработке ОИС в качестве служебного задания) способно заинтересовать потенциального работодателя в данном соискателе [7]. Данный аспект можно зафиксировать в «Паспорте компетенций», отражающем «...уровень развития надпрофессиональных навыков его обладателя...» [22]. Отмеченный в исследовании М. Р. Гафарова, М. Р. Сафиуллина, Л. А. Ельшина «инклюзивный рост территорий» в процессе их цифровой трансформации возможен благодаря усилению теории и практики вопросов управления событийным брендом креативных индустрий [4].

Список литературы

1. Балихина Д. О., Ершов Ю. М. Бренд-коммуникации в социальных медиа крымских виноделен // Вестник Воронежского государственного университета. Серия: Филология. Журналистика. – 2024. – № 1. – С. 91–94.
2. Белова Ю. В., Ермилова Д. Ю., Назарова Л. Р. Возможности дизайна в популяризации малых территорий – опыт проектной деятельности студентов // Сервис plus. – 2023. – Т. 17, № 1. – С. 115-124. – DOI 10.5281/zenodo.7992438.
3. Валькова Т. М., Глемейда А. С. Гастрономический туризм в Русской Арктике: туристские ресурсы территории // Географическая среда и живые системы. – 2023. – № 4. – С. 151–172. – DOI 10.18384/2712-7621-2023-4-151-172.
4. Гафаров М. Р., Сафиуллин М. Р., Ельшин Л. А. Цифровая трансформация как инструмент интенсификации инклюзивного экономического роста региона // Казанский экономический вестник. – 2021. – № 4(54). – С. 32–41.
5. Гумерова Г. И., Шаймиева Э. Ш. Креативные индустрии в экономике данных // Москва : Общество с ограниченной ответственностью "Издательство "КноРус". – 2025. – 176 с.
6. Гумерова Г. И., Шаймиева Э. Ш. Менеджмент организаций креативных индустрий в цифровой экономике: учебник. Москва: Общество с ограниченной ответственностью «Издательство "КноРус"», 2025. – 272 с.
7. Гумерова Г. И., Шаймиева Э.Ш., Манушин Д. В. Глава 8. Цифровые платформы для трудоустройства выпускников: управленческие аспекты на основе цифровизации образовательных организаций // Экономика и право: монография / гл. редактор Э. В. Фомин. – Чебоксары : Общество с ограниченной ответственностью «Издательский дом «Среда», 2023. – С. 131–143. – DOI 10.31483/g-107169.
8. Зона комфорта // Первое медиа о путешествиях и сервисе в России [Электронный ресурс]. – URL: <https://t.me/russiamatters> (дата обращения 18.08.2024).
9. Концепции развития творческих (креативных) индустрий и механизмов осуществления их государственной поддержки в крупных и крупнейших городских агломерациях до 2030 года // Утверждена Правительством Российской Федерации. Распоряжение от 20 сентября 2021 г. № 2613-р Москва [Электронный ресурс]. – URL: <http://static.government.ru/media/files/HEXNAom6EJunVlxBcJlAtAya8FAVDUfP.pdf> (дата обращения: 18.08.2024).

10. Карта рынка Event-услуг. [Электронный ресурс]. – URL: <https://maps.adpass.ru/maps/karta-rynka-event-uslug> (дата обращения: 18.08.2024)
11. Красовская, Н. В. Событийный маркетинг : учебное пособие для вузов // 3-е изд., испр. – Москва : Юрайт, 2024. – 116 с. // [Электронный ресурс]. – URL: <https://urait.ru/bcode/518856/p.49> (дата обращения: 08.08.2024).
12. Кредитование под залог интеллектуальной собственности // Московский инновационный кластер. Официальный сайт [Электронный ресурс]. – URL: <https://i.moscow/ip/credit> (дата обращения: 18.08.2024).
13. Официальный сайт фестиваля «Креатив на Волге» // [Электронный ресурс]. – URL: <https://kreativnavolge.ru> (дата обращения: 18.08.2024).
14. Официальный сайт «ПАРИ ФЕСТ» // [Электронный ресурс]. – URL: <https://parifest.ru> (дата обращения: 18.08.2024).
15. Официальный сайт гастрономического фестиваля «Сыр. Пир. Мир» // <https://xn--h1aalkeccb4g.xn--p1ai> (дата обращения: 18.08.2024).
16. Петрашевская Ю.В, Тенденции развития мирового рынка труда в сфере креативных индустрий // Региональная экономика и управление: электронный научный журнал. ISSN 1999-2645. – № 2(78). Номер статьи: 7805. Дата публикации: 21.04.2024. [Электронный ресурс]. – URL: <https://eee-region.ru/article/7805> (дата обращения: 18.08.2024)
17. Платформа НТИ // Официальный сайт [Электронный ресурс]. – URL: <https://platform.nti.work> (дата обращения: 18.08.2024).
18. Приказ об утверждении собирательной классификационной группировки видов экономической деятельности в области деятельности творческих (креативных) индустрий на основе Общероссийского классификатора видов экономической деятельности (ОКВЭД 2) ОК 029-2014 (КДЕС Ред. 2) // Утверждена приказом Министерства культуры РФ от 20.10.2023 № 2931 [Электронный ресурс]. – URL: <https://base.garant.ru/408100009> (дата обращения: 18.08.2024).
19. Региональный стандарт развития креативных индустрий // АСИ, Центр развития креативной экономики. – М., 2023. – 58 с.
20. Регионы России в фокусе событийной индустрии // Национальное конгресс-бюро. 02.2020. 42 с. [Электронный ресурс]. – URL: <https://russiacb.com/upload/iblock/50a/50a2d36363b33ac7cd30eb28676bec5d.pdf> (дата обращения: 18.08.2024).
21. Росмолодежь. Гранты // Федеральное агентство по делам молодежи (Росмолодежь) // [Электронный ресурс]. – URL: <https://fadm.gov.ru/directions/grant> (дата обращения: 18.08.2024).
22. Россия – страна возможностей. Мои мягкие навыки развиты на 10 из 10, и это подтверждено экспертами // [Электронный ресурс]. – URL: <https://t.me/stranavozmojnostey> (дата обращения: 18.08.2024).
23. Стартап как диплом // Министерство науки и высшего образования РФ. Официальный сайт [Электронный ресурс]. – URL: <https://minobrnauki.gov.ru/press-center/news/nauka-i-obrazovanie/25900> (дата обращения 18.08.2024).
24. Теслер Ю. А., Теличенко В. И. Фирменный стиль и идентичность парков / Ю. А. Теслер, // Components of Scientific and Technological Progress. – 2023. – № 9(87). – С. 12–16.

25. Товарные знаки. Поиск // Роспатент. Официальный сайт [Электронный ресурс]. – URL: <https://searchplatform.rospatent.gov.ru/trademarks> (дата обращения: 18.08.2024).

26. Трофимова Н. Н. Ключевые проблемы управления человеческим капиталом в организациях МІСЕ-индустрии // Экономика и управление: проблемы, решения. – 2024. – Т. 2, № 1(144). – С. 28–33. – DOI 10.36871/ek.ur.p.g.2024.01.02.004.

27. Федеральный закон от 08.08.2024 № 330-ФЗ «О развитии креативных (творческих) индустрий в Российской Федерации» // Официальное опубликование правовых актов [Электронный ресурс]. – URL: <http://publication.pravo.gov.ru/document/0001202408080136> (дата обращения: 18.08.2024)