Как цитировать: Цифровые технологии и право: сборник научных трудов IV Международной научно-практической конференции (г. Казань, 19 сентября 2025 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2026. 336 с. EDN: VMNZYI. http://dx.doi.org/10.21202/978-5-8399-0906-9_3 – 1 CD-ROM. – Загл. с титул. экрана. – Текст: электронный.

For citation: Digital Technologies and Law: collection of scientific papers of the IV International Scientific and Practical Conference (Kazan, 2025, September 19) / I. R. Begishev, E. A. Gromova, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 3. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2026. 336 p. EDN: VMNZYI. http://dx.doi.org/10.21202/978-5-8399-0906-9_3 – 1 CD-ROM. – Title from the title screen. – Text: electronic.

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
IV Международной научно-практической конференции

19 сентября 2025 г.

г. Казань

В шести томах

Том 3

Казань ▪ КИУ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ▪ 2026

Digital technologies and law

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

2025, September 19

Kazan

In 6 volumes

Volume 3

Казань ▪ KIU "POZNANIYE" PUBLISHERS ▪ 2026

УДК 004:34(063)
ББК 67с51я43
Ц75

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

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. Тимирясова;

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 IV Международной научно-практической конференции** (г. Казань, 19 сентября 2025 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2026. 336 с. EDN: VMNZYI. http://dx.doi.org/10.21202/978-5-8399-0906-9_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 978-5-8399-0910-6
ISBN 978-5-8399-0906-9 (Том 3)

Вошедшие в сборник научные труды приурочены к IV Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 19 сентября 2025 г. в Казани в рамках Международного форума Kazan Digital Week 2025, 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 представленного тома систематизированы по современным трендам развития цифровых технологий в системе теоретико-исторических правовых наук, публично-правовых и частноправовых отношений. В рамках указанных секций рассматриваются вопросы цифрового суверенитета, трансформации публичной власти и государственного управления в условиях цифровизации, теоретико-правовых оснований формирования цифрового государства и информационной безопасности и др.

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 978-5-8399-0910-6
ISBN 978-5-8399-0906-9 (Том 3)

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов IV Международной научно-практической конференции

19 сентября 2025 г.
г. Казань

В шести томах
Том 3

Под редакцией И. Р. Бегишева, Е. А. Громовой, 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. Загретдинова*

Дата подписания к использованию: 07.07.2026. Объем издания 4,5 Мб. Тираж 11 экз. Заказ № 11/2026.
ISBN 978-5-8399-0906-9

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

UDC 004:34(063)
LBC 67с51я43

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

Digital Technologies and Law: collection of scientific papers of the IV International Scientific and Practical Conference (Kazan, 2025, September 19) / I. R. Begishev, E. A. Gromova, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 3. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2026. 336 p. EDN: VMNZYI. http://dx.doi.org/10.21202/978-5-8399-0906-9_3 – 1 CD-ROM. – Title from the title screen. – Text: electronic.
ISBN 978-5-8399-0910-6
ISBN 978-5-8399-0906-9 (Vol. 3)

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

The scientific works included in the collection are tied with the 4th International scientific-practical conference "Digital Technologies and Law", which was held on September 19, 2025 in Kazan as part of Kazan Digital Week 2025 International Forum, organized by the Russian Government jointly with the Republic of Tatarstan Cabinet of Ministers.

The conference discussed a wide range of theoretical and methodological, practice-oriented, interdisciplinary and sectoral issues related to the priorities in the legal regulation of digital technologies, regulatory control over the digital environment, and prospective impact 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 law relations. They consider the issues of introducing digital technologies into forensic expertise, the institution of digital (electronic) evidence, automation of criminal proceedings, as well as other problems of digitalization of criminal legislation and law enforcement practice.

The ideas and proposals reflected in the 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, lawmakers and law-enforcers, government officials and participants in the real sector of the economy. These include developers and manufacturers of products based on digital technologies, young researchers – students, undergraduates, and postgraduates, to all those interested in the mutual influence of digital technologies and law

UDC 004:34(063)
LBC 67с51я43

ISBN 978-5-8399-0910-6
ISBN 978-5-8399-0906-9 (Vol. 3)

Scientific publication

DIGITAL TECHNOLOGIES AND LAW

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

2025 September 19
Kazan

In 6 volumes

Volume 3

I. R. Begishev, E. A. Gromova, 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: 07.07.2026. Volume of the publication 4.5 Mb. Number of copies: 11. Order No. 11/2026.
ISBN 978-5-8399-0906-9

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. Бегишев, 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. Тимирясова;

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);

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. Тимирясова

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);

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

Цифровые технологии в системе уголовно-правовых отношений

УДК 343.9

Ф. Г. Аминев,
доктор юридических наук, профессор,
профессор кафедры криминалистики Института права
Уфимского университета науки и технологий,
Заслуженный юрист Республики Башкортостан,
академик РАЕН

По вопросу внедрения цифровых технологий в судебно-экспертную деятельность

Аннотация. Показано, что в условиях сложной криминогенной обстановки в стране, необходимы дальнейшие усилия по внедрению высокотехнологичных средств и методов в судебно-экспертную деятельность. Рассмотрены возможности использования средств и методов цифровизации (автоматизация процессов, внедрение инновационного оборудования, инструментов обработки больших данных) в производстве различных видов судебно-экспертных исследований: молекулярно-генетических, технико-криминалистических исследований документов и других. Представлены разработанные автором рекомендации по оптимизации внедрения инновационных цифровых технологий в работу судебного эксперта.

Ключевые слова: машинное обучение, цифровые технологии, экспертные методики, искусственный интеллект, судебно-экспертная деятельность

F. G. Aminev,
Doctor of Law, Professor,
Professor of the Department of Criminalistics
at the Institute of Law Ufa University of Science and Technology,
Honored Lawyer of the Republic of Bashkortostan,
Academician of the Russian Academy of Natural Sciences

On the issue of introducing digital technologies into forensic expertise

Annotation. It is shown that in the conditions of a complex criminogenic situation in the country, further efforts are needed to introduce high-tech tools and methods into forensic expertise. The possibilities of using the means and methods of digitalization (automation of processes, introduction of innovative equipment, tools for processing big data) in the production of various types of forensic research: molecular genetic, technical and forensic studies of documents and others are considered. The recommendations developed

by the author on optimizing the implementation of innovative digital technologies in the work of a forensic expert are presented.

Keywords: machine learning, digital technologies, expert techniques, artificial intelligence, forensic expertise

Благодарности. Исследование выполнено за счет гранта Российского научного фонда № 24-28-00834, https://rscf.ru/project/24-28-00834

Введение. Об использовании цифровых технологий в криминальных целях свидетельствует официальная статистика: из «1 991 258 преступлений, зарегистрированных в 2024 году, 765 365 преступлений (40 % от общего количества) совершено с использованием информационно-телекоммуникационных технологий» [1]. Такое тревожное положение обусловливает необходимость интеграции инновационных цифровых технологий в практику борьбы с преступностью в том числе в судебно-экспертную деятельность. Цифровые технологии открывают новые возможности для производства судебно-медицинских диагностических исследований, извлечения цифровой информации и восстановления утраченных электронных данных, производства и интерпретации результатов молекулярно-генетических исследований и т.д. Кроме того, автоматизированные системы управления и поиска при производстве судебной экспертизы сокращают временные затраты на проведение исследований и снижают вероятность ошибок вследствие человеческого фактора. А использование методов компьютерного распознавания образов с применением искусственного интеллекта значительно улучшают процедуру идентификации объектов судебной экспертизы.

Однако внедрение современных цифровых разработок в практику сопровождается рядом проблем. В связи с этим правильным считаем высказывание А. В. Варданяна, рекомендующим проводить методические исследования так, чтобы они были не только теоретическими, но и «воплощали в себе также и результаты эмпирического анализа, практическую апробацию и внедрение» [6. С. 159].

Основная часть. Во внедрении цифровых технологий в судебную экспертизу достигнуты определенные успехи. Так, применяются: комплексы «3Д-моделирования для фиксации и экспертного исследования мест происшествий; компьютерные системы искусственного интеллекта в почерковедческих экспертизах; нейронные сети – в формировании интегрированной автоматизированной системы с использованием искусственного интеллекта» [2. С. 25], «психофизиологические экспертизы с применением полиграфа» [3. С. 37] с применением магнитно-резонансного томографа и т.д.

Однако, к сожалению, приходится признать слабое внедрение инновационных цифровых технологий в повседневную практическую работу судебных экспертов, причиной чего является ряд проблем:

1. Одной из главных проблем успешного внедрения цифровых технологий является отсутствие возможностей по валидации и апробации новейших экспертных методик. Так, крайне актуальными являются исследования по разработке и совершенствованию экспертных методик исследований документов. В методике «с применением хроматографа и насадкой твердых проб для решения задачи (например, установление давности исполнения рукописного текста) из исследуемого объекта вырезаются три участка, содержащие штрихи рукописного текста длиной не менее 10 мм каждый. В то же время предпринимаются попытки с помощью высокотехнологичных методов избежать такого разрушения объекта и с применением ядерно-магнитной спектроскопии (ЯМР-метода) провести судебно-экспертное исследование» [7. С. 26], в котором «для проведения экспертного исследования отбираются пробы-вырезы (отверстия диаметром не более 0,6 мм), с использованием специального инструмента пробоподготовки («пробойника») на «открытых» участках объектов (бумаги исследуемого документа, ткани и других объектов) и участках «покрытых» тонером (непосредственно печатный текст), красителем нанесенной подписи и оттиска мастичной печати» [7. С. 147]. Но эта методика так и остается невалидированной и неапробированной и, соответственно, не внедренной в практику.

Такая же ситуация происходит в молекулярно-генетических исследованиях. Учеными-криминалистами совместно с учеными-генетиками г. Уфы предложен «оригинальный метод изотермической амплификации целевых фрагментов ДНК, положенный в основу методики выявления полиморфизма ДНК человека и других организмов, включая кошек и собак» [4. С. 19; 8]. И эта инновационная экспертная методика не используется судебными экспертами.

2. Недостаточное финансирование разработки новых судебно-экспертных методик.

3. Острой проблемой внедрения цифровых технологий в судебно-экспертную деятельность является консерватизм, а в некоторых случаях – страх применения новых технологических решений, Так, Уфимским университетом науки и технологий разработана «компьютерная программа идентификации личности по снипам (SNP-локусам) и обработке большого объема геномной информации с большим уровнем цифровизации (патент зарегистрирован 5 декабря 2022 года)» [5]. Тем не менее, она остается не внедренной.

4. Действующая нормативно-правовая регламентация не успевает адаптироваться к постоянно развивающимся цифровым технологиям (особенно, в области искусственного интеллекта, больших данных и т.д.). Например, не регламентированы четкие критерии оценки доказательств, полученных в результате применения 3D-моделирования, искуссвтеного интеллекта и др.).

5. Еще одной важной проблемой является ограниченные технические возможности разработанных программно-компьютерных систем: низкая разрешающая способность сканирующих средств 3D-моделирования при производстве судебных

экспертиз и исследований; малый объем данных, используемых при машинном обучении нейронной сети и др. И одной из причин данной проблемы видится в бюрократизировании процедур финансирования закупок, в ходе которых приходится тратить слишком много времени и сил для согласования приобретения новых инновационных средств и оборудования.

6. У судебных экспертов наблюдается недостаточный уровень знаний, умений и навыков эффективного применения передовых цифровых технологий при производстве судебных экспертиз. В рамках этой проблемы особо ярко выражена недостаточная мотивация сотрудников судебно-экспертных организаций (в виде высокой заработной платы, системы стимулов и поощрений и др.), которая лишает возможности принимать на работу в судебно-экспертную организацию компетентных лиц, обладающих специальными знаниями более высокого уровня компетентности (особенно, в сфере IT-технологий и искусственного интеллекта). Так как, таким высококвалифицированным специалистам в других сферах предлагаются гораздо большее денежное довольствие, и они, конечно же, выбирают работу не судебного эксперта, а IT-менеджера, инженера-компьютерщика в банках и коммерческих организациях.

Заключение. В целях успешной организации внедрения актуальных цифровых технологий предлагаем:

– переработать нормативно-правовые акты в целях регламентации применения современных цифровых технологий в судопроизводстве;

– необходимо проводить профессиональную подготовку и переподготовку судебных экспертов по овладению новейшими инновационными средствами и методами экспертного исследования. Требуется привлечение IT-специалистов для повышения уровня технологизации профессиональной подготовки судебных экспертов;

– постоянно повышать уровень цифровизации программного и технологического обеспечения судебной экспертизы с алгоритмами машинного обучения с использование больших данных (Big Data);

– улучшить материально-техническому обеспечение работы судебных экспертов.

Имеется уверенность, что рекомендованный комплекс мероприятий правового, научно-методического, кадрового и материально-технического характера позволит существенно повысить внедрение инновационных цифровых технологий в судебно-экспертную деятельность.

Список литературы

1. Состояние преступности в России за январь-декабрь 2024 года. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения 24 февраля 2025 г.).

2. Аминев Ф. Г. О проблемах внедрения инновационных естественнонаучных технологий в судебно-экспертную деятельность // Национальные и международные тенденции и перспективы развития судебной экспертизы: Сборник докладов Научно-практической конференции с международным участием, Нижний Новгород, 22–23 мая 2024 года. Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2024. С. 24-31.

3. Аминев Ф.Г., Гайнуллина С.М., Башкатов С.А. К вопросу повышения надежности психофизиологической экспертизы с применением полиграфа // Актуальные проблемы использования специальных знаний в уголовном, гражданском, арбитражном процессе и по делам об административных правонарушениях: сборник материалов XIII международной научно-практической конференции (Уфа, 25 октября 2024 г.) / Частное учреждение «Научно-исследовательский институт проблем правового государства». Уфа, 2024. С. 37-39.

4. Аминев Ф.Г. О некоторых актуальных направлениях использования современных технологий в правоприменительной практике // Высокотехнологичное право: современные вызовы: материалы IV Международной межвузовской научно-практической конференции (Москва-Красноярск, 17-20 февраля 2023 года). Т. Часть 1. Красноярский государственный аграрный университет. Красноярск, 2023. С. 16-21.

5. Аминев Ф.Г., Сагитова М.А., Чемерис А.В., Гарафутдинов Р.Р., Сагитов А.М., Анисимов В.А. SNPmod: Свидетельство о регистрации программы для ЭВМ 2022683416 05.12.2022. Заявка № 2022683187 от 28.11.2022. Федеральная служба по интеллектуальной собственности, 2022.

6. Варданян А.В. Современные проблемы использования специальных знаний в уголовном судопроизводстве // Юристъ-Правоведъ. 2019. № 2 (89). С. 158-163.

7. Плетень О.И., Плетень П.О. Внедрение современных достижений науки и техники в экспертную практику вневедомственных экспертов («Методика определения давности создания объекта, содержащего целлюлозу, методом импульсной ЯМР-спектроскопии») // Актуальные проблемы судебно-экспертной деятельности в уголовном, гражданском, арбитражном процессе и по делам об административных правонарушениях: материалы VI Международной научно-практической конференции 12-13 октября 2017 г. Уфа: РИЦ БашГУ, 2017. С. 142-149.

8. A new digital approach to SNP encoding for DNA identification / R.R. Garafutdinov, A.R. Sakhabutdinova, P.A. Slominsky, F.G. Aminev, A.V. Chemeris // Forensic Science International. 2020; V. 317. P. 110520. DOI: DOI: 10.1016/j.forsciint.2020.110520.

УДК 343

Е. Ю. Антонова,
доктор юридических наук, профессор,
Московский университет «Синергия»

Цифровая безопасность как объект уголовно-правовой охраны

Аннотация. Рассматривается вопрос об объекте преступлений, совершаемых с использованием цифровых технологий, или когда их местом выступают цифровые площадки. Отмечается, что цифровизация общественных отношений и появление новых киберугроз способствовали расширению перечня преступлений в сфере компьютерной информации и изменению интенсивности пенализации за счет добавления отягчающего признака «совершение преступления с использованием информационно-телекоммуникационных сетей». Цель исследования: выявить, какой объект ставится под угрозу причинения вреда (ущерба) в результате совершения преступлений в цифровом пространстве и (или) с использованием цифровых технологий.

Ключевые слова: цифровая безопасность, информационная безопасность; объект преступления; основной объект; дополнительный объект; компьютерная информация; информационно-телекоммуникационные сети

E. Yu. Antonova,
Doctor of Law, Professor,
Moscow University «Synergy»

Digital security as an object of criminal law protection

Abstract. The issue of the object of crimes committed using digital technologies, or when their place is digital platforms, is considered. It is noted that the digitalization of public relations and the emergence of new cyber threats have contributed to the expansion of the list of crimes in the field of computer information and a change in the intensity of penalization by adding the aggravating factor of «committing a crime using information and telecommunications networks». The purpose of the study: to identify which object is at risk of causing harm (damage) as a result of committing crimes in the digital space and (or) using digital technologies.

Keywords: digital security; information security; object of crime; main object; additional object; computer information; information and telecommunication networks

Введение. Объект преступления в доктрине уголовного права относится к числу наиболее разработанных и, вместе с тем, дискуссионных проблем. Новые реалии не упрощают, а скорее усложняют данный вопрос. В частности, научно-технический прогресс в информационной сфере, а также стремительная цифровизация общественных отношений способствовали появлению различных киберугроз. Это,

с одной стороны, привело к потребности установления уголовно-правовых запретов общественно опасных деяний, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий, но, с другой стороны, процесс этот происходит хаотично. Отсюда возникает вопрос о цифровой безопасности как объекте уголовно-правовой охраны. Ключевыми здесь являются следующие вопросы: что следует понимать под цифровой безопасностью, и в каких случаях таковая должна ставиться под охрану именно уголовного закона.

Основная часть. Данные вопросы особенно актуальны в связи с расширением в уголовном законе перечня компьютерных преступлений и изменением интенсивности пенализации некоторых составов преступлений путем включения конструктивного (криминообразующего) или отягчающего (квалифицирующего) признака – использование информационно-телекоммуникационных сетей (далее – ИТС) или совершение преступлений в данных сетях. В свою очередь это влечет за собой видоизменения в характеристике объекта преступлений, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий, автоматически они становятся многообъектными. При этом очевидно, что даже при идентичности формулировок смысловое значение данных признаков, с точки зрения института объекта преступления, не всегда совпадает даже в рамках системы преступлений, входящих в одну группу по признаку родового или видового объекта. Для примера обратимся к таким преступлениям как убийство, совершенное с публичной демонстрацией, в том числе в ИТС (п. «о» ч. 2 ст. 105 УК РФ) и склонение к самоубийству или содействие совершению самоубийства, совершенное в ИТС (п. «д» ч. 3 ст. 110^1 УК РФ). Родовым объектом данных преступлений является безопасность личности, видовым – жизнь и здоровье человека, основным непосредственным – жизнь человека. Публичная демонстрация процесса или результата убийства в ИТС, а равно склонение к самоубийству или содействие самоубийству в ИТС законодатель вынес в квалифицированный и особо квалифицированный состав. Какой же дополнительно объект претерпевает негативное воздействие при совершении данных преступлений в цифровом пространстве?

На наш взгляд, использование ИТС при совершении убийства, в первую очередь, негативно сказывается на общественной нравственности. Это следует, в том числе из пояснительной записки к закону, которым данный признак был установлен. В частности, в документе сказано, что убийство или иные преступления против личности, совершенные с публичной демонстрацией в ИТС (так называемые «треш-стримы»), возводят такое преступное поведение «в ранг допустимого и возможного для неограниченного круга лиц». Другими словами, такие деструктивные действия пропагандируются как норма, что оказывает негативное влияние именно на общественную нравственность, которая является составным элементом общественной безопасности в цифровом пространстве.

Во втором же случае под угрозу ставится информационная безопасность, которую применительно к названному составу преступления можно определить как состояние защищенности личности от внутренних и внешних информационных угроз, при котором обеспечивается реализация конституционных прав и свобод человека и гражданина. В рассматриваемом случае в ИТС распространяется контент, который направлен на причинение себе физического вреда (смерти), т.е. человек в цифровом (информационном) пространстве получает информацию, способную повлечь за собой необратимые последствия, а именно его смерть.

В научной литературе такие деяния именуются «онлайн-сопровождением», т. е. когда Интернет используется для «поиска, загрузки или обмена информацией, связанной с физическим самоповреждением», в том числе суицидальным намерением [13].

Рассматриваемый признак, как уже отмечалось, появляется все в большем количестве составов преступлений. Причем в отдельных случаях законодатель устанавливает данный признак дважды (например, ч. 1^1 и п. «б» ч. 2 ст. 258^1; ч. 2 и п. «б» ч. 3 ст. 260^1 УК РФ). Это ведет к сложностям в процессе квалификации преступлений [2. С. 164–169; 3. С. 23–27]. В некоторых же случаях законодатель пока не решается вводить его. Это касается, например, преступлений сексуальной направленности. Вместе с тем, все чаще в научной литературе [9. С. 68–83; 1. С. 450–459] можно встретить рассуждения о цифровом насилии в целом, и цифровом сексуальном насилии, в частности. Полагаем, что установление соответствующего признака в преступлениях сексуально направленности – это дело времени.

Возвращаясь к объекту преступлений, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий, отметим, что в научной литературе употребляются различные термины для обозначения такового. В частности, ученые говорят о «цифровой безопасности», «кибербезопасности», «онлайн-безопасности», «информационной безопасности», «компьютерной безопасности».

По мнению С.В. Маликова, основной объект преступлений с использованием информационных технологий – общественные отношения, обеспечивающие безопасность в сфере компьютерной информации [5. С. 95].

Е.А. Русскевич предлагает дополнить перечень объектов, подпадающих под уголовно-правовую охрану (ч. 1 ст. 2 УК РФ), информационной безопасностью [8. С. 14, 24–25].

Есть и более глобальное определение объекта посягательств в цифровом пространстве. Так, Р.Г. Дремлюга считает, что объектом уголовно-правовой охраны является цифровая экономика и информационное общество [4. С. 82].

Для специалистов в области компьютерных технологий термин «кибербезопасность» обычно относится к политикам, процессам и практикам, предпринимаемым для предотвращения несанкционированного доступа к данным, сетям и системам [11. P. 76–92].

Понятия «кибербезопасность» и «информационная безопасность» зачастую используются как синонимы и определяются как «состояние защищенности обрабатываемых, хранимых и передаваемых данных от незаконного ознакомления, изменения и уничтожения, а также состояние защищенности информационных ресурсов от воздействий, направленных на то, чтобы нарушить их работоспособность» [7. С. 243]. А ключевую задачу кибербезопасности видят в предотвращении вредоносных кибератак на информационные системы, сети и программы [7. С. 243].

Так, учеными подчеркивается, что важным аспектом онлайн-безопасности является защита пользователей от мошеннических веб-сайтов и фишинговых атак (такой преступный технический механизм, который используется для кражи личных данных и учетных данных финансовых счетов) [10. P. 69–82]. Например, в марте 2020 года была выявлена фишинговая атака на Всемирную организацию здравоохранения (ВОЗ). Группа киберзлоумышленников запустила вредоносный веб-сайт, имитирующий внутреннюю систему электронной почты ВОЗ, с целью украсть пароли у сотрудников ВОЗ. Атака оказалась безуспешной, но подчеркнула уровень сложности некоторых фишинговых атак [14].

В уголовном праве об информационной безопасности предлагают вести речь, когда возникает потребность защиты сохранности и конфиденциальности а) данных, хранящихся на электронных и бумажных носителях; б) информационно-коммуникационных систем, сайтов, информационных ресурсов и объектов критической информационной инфраструктуры, а также защиты граждан и общества от распространения заведомо ложной информации, социально-опасной или недостоверной информации [6. С. 14].

Полагаем, что понятие «цифровой безопасности» является более емким, охватывающим более полный спектр аспектов, подпадающих под охрану уголовного закона. Предлагаем понимать под «цифровой безопасностью» в сфере уголовно-правовых отношений состояние защищенности личности, общества и государства от общественно опасных деяний, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий или в сфере компьютерной информации. При этом в качестве основного объекта цифровая безопасность выступает только в случае совершения компьютерных преступлений. Если же цифровые технологии используются в качестве способа, орудия / средства совершения преступления или местом совершения преступления выступает цифровая площадка, цифровая безопасность может выступать лишь в качестве дополнительного или факультативного объекта.

Заключение. Считаем, что, прежде чем конструировать уголовно-правовые нормы, направленные на защиту цифровой безопасности необходимо смоделировать характер возможных угроз.

Для этого необходимо ответить на вопросы: какую информацию мы хотим защитить, от кого мы хотим ее защитить, каковы их возможности, насколько вероятно,

что нам придется ее защищать, и каковы могут быть последствия, если мы этого не сделаем [12. P. 405–425]. Последовательность решения данных вопрос нужна, в том числе для решения вопроса о характере и степени общественной опасности соответствующего деяния, ведь именно от этого зависит и вопрос о целесообразности охраны соответствующих объектов и криминализации деяния. Вполне возможно, что в отдельных случаях достаточными будут менее репрессивные меры (административно-правовые или гражданско-правовые) воздействия на нарушителей, а в каких-то – соответствующая криминализация является излишней.

Список литературы

1. Антонова Е. Ю. Сексуальное насилие в эпоху цифровизации: вопросы правовой оценки // Всероссийский криминологический журнал. 2024. Т. 18, № 5. С. 450-459. DOI 10.17150/2500-4255.2024.18(5).450-459.

2. Антонова Е. Ю. Уголовная политика в сфере охраны особо ценных диких животных и водных биологических ресурсов // Байкальский природоохранный форум: сборник статей I (X) Международной научно-практической конф., Иркутск, 09.06.2023. Иркутск: Иркутский юридический институт (филиал) Университета прокуратуры РФ, 2023. С. 164-169.

3. Антонова Е. Ю. Норма об ответственности за посягательства на особо ценные растения и грибы: некоторые вопросы законодательной техники // Енисейские политико-правовые чтения: сборник научных статей по материалам XV Всероссийской научно-практической конференции, Красноярск, 29–30 сентября 2023 года. Красноярск: Красноярская региональная общественная организация «Общественный комитет по защите прав человека», 2023. С. 23-27.

4. Дремлюга Р. Г. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение. М.: Юрлитинформ, 2022. 328 с.

5. Информационные технологии в уголовно-правовой сфере: монография / О. Ю. Антонов, А. И. Бастрыкин, А. А. Бессонов [и др.]. Москва: Юнити Дана, 2023. 279 с.

6. Лихачев Н. А. Уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности: законодательный, правоприменительный и доктринальный аспекты: дис. … канд. юрид. наук: 5.1.4. Краснодар, 2024. – 237 с.

7. Риски цифровизации: виды, характеристика, уголовно-правовая оценка: монография / отв. ред. Ю.В. Грачева. Москва: Проспект, 2022. 272 с.

8. Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: автореф. дис. … д-ра юрид. наук: 12.00.08. М., 2020. 52 с.

9. Сидоренко Э. Л. Цифровое насилие в отношении детей: понятие, виды и особенности квалификации // Lex Russica (Русский закон). 2024. Т. 77, № 12(217). С. 68-83. DOI 10.17803/1729-5920.2024.217.12.068-083.

10. Alsharnouby M., Alaca F., Chiasson S. Why phishing still works: User strategies for combating phishing attacks // International Journal of Human-Computer Studies. 2015. Vol. 82. P. 69-82. DOI: 10.1016/j.ijhcs.2015.05.005.

11. Dupont B., Whelan C. Enhancing relationships between criminology and cybersecurity // Journal of Criminology. 2021. Vol. 54(1). P. 76-92. DOI: 10.1177/00048658211003925.

12. Kindynis, T., Fleetwood, J. Information security for criminological ethnographers // Crime, Media, Culture. 2024. Vol. 20(4). P. 405-425. DOI: 10.1177/17416590231219746.

13. Mateos-Pérez, E., Martínez-Bacaicoa, J., Wachs, S., Gámez-Guadix, M. Longitudinal associations of online self-harm with online victimization through cyberbullying, hate speech, online grooming and nonconsensual sexting // Journal for the Study of Education and Development. 2025. Vol. 0(0). DOI: 10.1177/02103702251352943.

14. Niki O, Saira G, Arvind S, Mike D. Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that // Digital Health. 2022. Vol. 8. DOI: 10.1177/20552076221104665.

УДК 343.2/.7

Е. Г. Арефинкина,
кандидат юридических наук,
Сочинский институт (филиал)
Российского университета дружбы народов
имени Патриса Лумумбы

Уголовное право в условиях цифровизации: современное состояние и перспективы развития

Аннотация. Цель настоящей работы – анализ влияния цифровой трансформации современного российского общества на уголовное право, выявление вызовов современной преступности и предложение путей модернизации уголовного законодательства для эффективной защиты общественных отношений в виртуальном пространстве. Безусловно, цифровизация улучшает качество жизни, упрощая доступ ко многим ресурсам, в том числе и правовым, но она также порождает и новые риски, к которым относится киберпреступность, ставшая в короткие сроки трансграничной, сохраняющая максимальную анонимность и при этом масштабность. Необходимо констатировать отсутствие в современном уголовном законодательстве действенной защиты от роста угроз со стороны искусственного интеллекта и реальных механизмов охраны "цифровой личности". Необходимы скорейшие изменения, которые будут действовать на опережение: грамотный контроль, в том числе, и уголовно-правовой, за интеграцией в правовую сферу цифровых нововведений, поиск грамотного баланса между традиционными нормами права и вновь возникшими цифровыми институтами.

Ключевые слова: уголовное право, цифровизация, киберпреступность, традиционные нормы, цифровой след, механизмы охраны, искусственный интеллект

E. G. Arefinkina,
Candidate of Law, head of the Criminal Law and Process
Department of Sochi Institute (branch) of the Russian University of Peoples'
Friendship named after Patrice Lumumba

Criminal law in the context of digitalization: current status and development prospects

Abstract. The purpose of this article is to analyse the impact of the digital transformation of modern Russian society on criminal law, identify the challenges of modern crime, and propose ways to modernise criminal legislation for the effective protection of public relations in virtual space. Digitalisation undoubtedly improves quality of life by simplifying access to many resources, including legal ones. However, it also creates new risks, such as transnational cybercrime, which maintains maximum anonymity and scale. It is important to note that modern criminal law does not currently offer adequate protection

against the growing threats posed by artificial intelligence and that there are no real mechanisms in place to protect "digital identity". Urgent changes are needed that will act proactively: competent control, including criminal law control, over the integration of digital innovations into the legal sphere, and the search for a competent balance between traditional legal norms and newly emerging digital institutions.

Keywords: criminal law, digitalisation, cybercrime, traditional norms, digital footprint, protection mechanisms, artificial intelligence.

Введение. Цифровизация общества представляет собой глобальный процесс трансформации, затрагивающий все сферы человеческой деятельности, включая правовую. Безусловно, новейшие технологии улучшают качество жизни человека. Делают проще и профессиональную работу юриста. Сегодня с помощью соответствующих правовых систем очень удобно отслеживать последние изменения в действующем законодательстве или знакомиться с судебной практикой по сложным вопросам, состоявшимися судебными актами по различным категориям дел и пр. Это те новшества, о которых специалисты прошлых лет могли только мечтать [10]. Внедрение информационных технологий в различные сферы общественной жизни, появление новых видов технических средств, формирование информационного пространства в качестве платформы, обеспечивающей гармоничное взаимодействие между различными субъектами юридических отношений, а также развитие искусственного интеллекта - реалии современного информационного (сетевого) общества [2. С. 39]. С внедрением искусственного интеллекта, блокчейна и массивов данных в рутину классические правовые подходы встречают серьезные препятствия. Правила, рассчитанные на физическую реальность, плохо подходят для онлайн-мира, где зарождаются новые угрозы – хакерские вторжения, кражи электронных ценностей, подтасовка информации. Основная проблема на сегодняшний день на настоящем этапе развития законодательства и права – необходимость четкого и недвусмысленного регулирования, в том числе и уголовно-правовыми средствами, цифровых отношений во многих сферах жизни и деятельности человека.

Основная часть. Уголовное право сегодня – это итог долгой эволюции идей, норм и их использования на практике. Русскевич Е.А. точно подмечает, что цифровизация связей в обществе обнажает глубокие несоответствия между "виртуальной" преступностью нашего века и старыми методами борьбы с ней [8. С. 586]. На сегодняшний день «интернет вещей» (Internet of Things, IoT) лидирует во всех сферах жизнедеятельности человека. Более того, можно констатировать, что в настоящее время мы уже оказались свидетелями перехода от интернета людей к интернету вещей. Ожидается, что количество подключенных к сети Интернет-устройств по всему миру увеличится почти вдвое: с 19,8 млрд в 2025 году до более чем 40,6 млрд IoT-устройств к 2034 году [11]. Чем может быть опасен интернет вещей и какие формы преступности будут развиваться, в связи с этим? Ответ на этот вопрос

лежит на поверхности. Смартфон, умные гаджеты и устройства собирают информацию о состоянии здоровья человека, его передвижениях, привычках, увлечениях, предпочтениях, покупках, круге общения и жизненных привычках и пр. "Цифровой след" сегодня — это уникальный идентификатор, раскрывающий личность человека. Подобно дактилоскопии, которая позволяет точно установить лицо по отпечаткам пальцев, оставляемый нами «цифровой след» очень многое может рассказать о нас самих, по сути, это универсальные устройства для отслеживания их обладателя, несанкционированный доступ к данной информации преступников сделает человека абсолютно уязвимым и не защищенным. Подделать отпечатки пальцев на сегодняшний день практически невозможно, накопленный опыт и знания криминалистов не позволят это сделать, а вот возможности полной защиты личности, в том числе от фальсификации цифровых следов, не ясны научно и не доказаны.

Согласно постановлению Пленума ВС РФ от 15.12.2022 N 37 «к числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом» [6], поэтому IoT-устройства вполне можно отнести к числу компьютерных устройств [3. С. 127]. Эти устройства могут как содействовать правоохранительным органам в раскрытии преступлений, ибо сами по себе являются источником ценной криминалистической информации, так и помогать злоумышленнику искусственно создавать цифровое алиби, путем настройки умных устройств на создание видимости присутствия в каком-либо месте в нужное время и т.д.

Следует констатировать, что в настоящее время обеспечение защиты общественных отношений, формирующихся в процессе реализации прав человека в виртуальной среде, а также в области использования цифровых активов, криптовалют и иных аналогичных объектов, сопряжено со значительными трудностями. Инструментарий уголовно-правовой защиты во многих случаях оказывается неэффективным при противодействии посягательствам на отношения, опосредуемые современными информационно-коммуникационными технологиями. В частности, хотя неправомерный доступ к личной странице другого лица в социальной сети и может быть квалифицирован как преступление в соответствии с УК РФ, правовая оценка и квалификация создания и эксплуатации подобной страницы от имени другого лица без получения на то его согласия представляется крайне затруднительной. Между тем, подобного рода действия способны причинить существенный вред правам

и охраняемым законом интересам личности, а также оказать влияние на принятие решений, имеющих юридически значимые последствия.

Аналогичным образом, нормы действующего уголовного законодательства не содержат четкого ответа на вопрос о квалификации применения технологий реконструкции лица другого человека в режиме реального времени. Зачастую технологии «подмены лица» используются в ходе различных провокационных звонков, осуществляемых посредством аудио- и видеосвязи. Новейшие технологические разработки также позволяют использовать образ лица другого человека при производстве тех или иных компрометирующих материалов или даже материалов порнографического характера. Подобные материалы, получив широкое распространение в социальных сетях, способны серьезно нарушить права потерпевшего и повлечь за собой тяжкие последствия разнообразного характера.

Современный искусственный интеллект, проанализировав даже секундные образцы речи, обладает способностью создавать убедительные дипфейки, с высокой точностью воспроизводя интонационные особенности и тембр голоса конкретного человека. Эксперты прогнозируют, что в ближайшем будущем получит распространение практика осуществления видеозвонков с одновременным синтезом речи и изображения звонящего лица [5, 9]. То есть использование технологии искусственного интеллекта сегодня уже превратилась в один из способов совершения множества преступлений. К сожалению, законодательная регламентация в большинстве случаев отстает от тенденций развития преступности, так как действует не на опережение, а постфактум. На сегодняшний день в главе 28 УК РФ «Преступления в сфере компьютерной информации» отсутствуют составы, которые бы охватывали преступления, совершенные с использованием новых технологий. Безусловно, уголовное право и законодательство должно меняться последовательно, поэтапно и постепенно, учитывая современные реалии и технологии. Однако технологий искусственного интеллекта на сегодняшний день стали серьезной угрозой, так как превращаются в проверенный способ совершения целого ряда преступлений. Недавно в УК РФ были внесены поправкам, связанные с использованием информационно-телекоммуникационной сети Интернет. Вместе с тем, давно уже назрела необходимость в качестве квалифицирующего признака и обстоятельства, отягчающего уголовную ответственность, указать в законодательстве также и применение злоумышленниками технологий искусственного интеллекта [1. С. 67].

Согласно данным МВД России, в 2024 году зарегистрировано 765,4 тыс. киберпреступлений, что на 13,1 % больше, чем в 2023 году, и составляет 40% от общего числа преступлений. В первой половине 2025 года общее число преступлений в сфере компьютерной информации сократилось на 22,3 %, однако ущерб от киберпреступлений вырос на 30 % с начала года, достигнув 81 млрд руб. по итогам 2024 года и превысив 80 млрд руб. за 5 месяцев 2025 года. Кроме того, в 2024 году

зафиксировано более 1,8 млрд кибератак, многие из которых политически мотивированы [4].

Обобщив все имеющиеся данные в литературе, а также сложившейся практике, официальную статистику ведомственных органов, можно сказать, что преступность с использованием информационно-коммуникационных технологий на сегодняшний день характеризуется следующим.

Во-первых, в информационной сети она давно уже стала трансграничной и стерла территориальные границы: огромные расстояния между преступником и потерпевшим, находящимся в другой части земного шара, давно перестали быть проблемой, сети позволяют в физическом плане дистанцироваться как от пострадавших, так и правоохранительных органов.

Во-вторых, в сети злоумышленнику проще сохранять свою анонимность и чувство личной безопасности. Все это априори дает явное и серьезное преимущество преступнику. Человек, общающийся с Вами в виртуальной среде, по факту может оказаться кем угодно. К тому же, виртуальная среда снимает и многие психологические, культурные, личностные, языковые барьеры с помощью существующих цифровых технологий.

В-третьих, преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий, как никаким другим, свойственна масштабность. Виртуальный мир дает уникальную возможность цифрового воздействия на огромное количество потерпевших.

В-четвертых, благодаря особенностям архитектуры глобальной сети и специфике вредоносных программ цифровые преступления могут обернуться колоссальными последствиями как финансового, так и техногенного характера.

В-пятых, появление новых технологий в широком доступе неизбежно порождают новую волну преступности. Кроме того, постоянно совершенствуется и сама цифровая преступность, причем, в этом она пока однозначно идет на несколько шагов впереди соответствующих правоохранительных структур, которые осуществляют с ней борьбу.

И наконец, в-шестых, компьютерная преступность сегодня практически не поддается нормальному статистическому учеты, что связано с ее глобальным характером, разнообразием форм, недостатками действующего законодательного регулирования во многих странах мира, нежеланием потерпевших обращаться в правоохранительные органы из-за сложности установления виновных и низкой доказуемости и раскрываемости такого рода преступлений.

Активное развитие нейросетей и искусственного интеллекта, вероятнее всего, приведет к внедрению в юридическую практику такого понятия, как «цифровая личность», что принципиально изменит сферу уголовно-правовых отношений. Очевидно, что цифровизация становится неотъемлемой частью нашей жизни. В новых условиях многократно начинают увеличиваться и уголовно-правовые риски. Ведь

научно-технический процесс уже привел к появлению новых форм преступности в сфере компьютерной информации. В ближайшей перспективе вполне ожидаем ее рост как среди мошенничеств с использованием информационных систем, кибератак, взлома информационных государственных ресурсов и пр., так и в сфере активно развивающихся нейросетей, искусственного интеллекта. Уголовное право должно работать на опережение, а не меняться постфактум. Поэтому о совершенствовании механизма уголовно-правовой охраны в недалеком будущем нужно думать уже сейчас, анализируя различные научные теоретические подходы, сложившуюся практику, а также тенденции развития цифровой преступности.

В будущем фокус внимания юриста должен будет сместиться в сферу управления юридическими рисками, просто информировать о них или предложить различные варианты действий будет уже недостаточно, нужно будет продумывать оптимальный алгоритм решения сложной юридической ситуации в том числе и уголовно-правовыми способами. Реальную угрозу может представлять ошибочный подход к адаптации правовой системы и юридических процедур к новым цифровым реалиям: как отсутствие четкой и последовательной регламентации серьезных юридических процедур особенно в сфере уголовного права и процесса, так и отрицание того факта, что новые компьютерные технологии гораздо быстрее человека могут анализировать огромные массивы данных, в том числе и связанные с совершением преступлений, предлагать свои версии и план расследования, варианты подбора наказания и пр. Иными словами, нельзя упускать из виду тот факт, что современные технологии и нейронные сети, неся в себе множество рисков и угроз, связанных с масштабным развитием киберпреступности, одновременно с этим могут оказывать и реальную помощь правоохранительным органам в противодействии ей. Ключевое значение имеет правильное и грамотное использование их потенциала во благо, в том числе для развития и совершенствования уголовного законодательства, а также контроль за доступом к цифровым доступам и цифровым следам.

Список литературы

1. Ермолович Я.Н. Новое обстоятельство, отягчающее наказание, в уголовном законодательстве России (научно-практический комментарий к Федеральному закону «О внесении изменений в Уголовный кодекс Российской Федерации» от 8 августа 2024 года N 218-ФЗ) // Право в Вооруженных Силах. 2025. N 1. С. 67–74.

2. Иерархии и сети: власть и закон: Монография / И.А. Исаев, А.В. Корнев, С.В. Липень. М.: Проспект, 2022. С. 38–40.

3. Коринь А.В. Интернет вещей: криминалистические аспекты // Актуальные проблемы российского права. 2025. N 2. С. 125–133.

4. МВД РФ. Состояние преступности. https://мвд.рф/folder/101762. (дата обращения: 03.09.2025).

5. Отраднов Р. ЦБ: мошенники научились имитировать голоса родных потенциальной жертвы. URL: https://rg.ru/2024/01/17/cb-moshenniki-stali-chashche-imitirovat-golosa-rodnyh-potencialnoj-zhertvy.html (дата обращения: 03.09.2025).

6. Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 "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" // СПС "КонсультантПлюс".

7. Робот-адвокат: как юристам не остаться без работы [Электронный ресурс] // Forbes. URL: https:// www.forbes.ru/kompanii/343269-robot-advokat-kak-yuristamne-ostatsya-bez-raboty. (дата обращения: 12.08.2025).

8. Русскевич Е.А., Дмитренко А.П., Кадников Н.Г. Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации // Вестник Санкт-Петербургского университета. 2022. Право 3. С. 585-597.

9. Щепетильников В.Н. Уголовно-правовые меры борьбы с преступлениями, совершаемыми с использованием технологий искусственного интеллекта // Ex jure. 2025. N 1. С. 17 -183.

10. Арефинкина, Е. Г. Цифровизация юридической профессии: риски, потребности и перспективы реформирования юридического образования / Е. Г. Арефинкина // Технологии XXI века в юриспруденции : Материалы Пятой международной научно-практической конференции, Екатеринбург, 19 мая 2023 года. – Екатеринбург: АНО «Центр содействия развитию криминалистики «КримЛиб»», 2023. – С. 12-20. – EDN OIOTPA.

11. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 // URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (дата обращения: 21.08.2025).

УДК 34.343

А. С. Артемьева,
адъюнкт,
Санкт-Петербургский Университета МВД России

Биометрическая экосистема криминологической безопасности в условиях экономики данных

Аннотация. На фоне реализации стратегий цифровой трансформации государственного управления и развития информационного общества в условиях перехода на экономику данных в статье анализируются действующие направления ведомственной программы цифровой трансформации органа исполнительной власти в лице МВД России. Обращается внимание на необходимость трансформации непосредственной оперативно-служебной деятельности. Автором предлагается расширить перечень мероприятий программы, включив в них создание и внедрение биометрической экосистемы, способствующей обеспечению криминологической безопасности. Целью статьи является выдвижение идей и предложений по усовершенствованию деятельности органов внутренних дел, связанной с защитой личности, общества и государства от преступных посягательств и угроз таких посягательств, за счет комплексной автоматизации работы с большими объемами биометрических данных на основе искусственного интеллекта и созданию инфраструктуры, отвечающей по своим технологическим возможностям уровню современного развития науки и техники.

Ключевые слова: биометрические персональные данные, экосистема, информационные технологии, цифровая трансформация, экономика данных, криминологическая безопасность

A. S. Artemeva,
postgraduate,
Saint Petersburg University of the Ministry of the Interior of Russia

Biometric ecosystem of criminological security in the data economy

Abstract. Against the backdrop of the implementation of strategies for the digital transformation of public administration and the development of the information society in the context of the transition to a data-driven economy, the article analyzes the current directions of the departmental program for the digital transformation of the executive authority represented by the Ministry of Internal Affairs of the Russian Federation. Attention is drawn to the need for the transformation of direct operational and service activities. The author proposes to expand the list of program activities by including the creation and implementation of a biometric ecosystem that contributes to ensuring

criminological security. The purpose of this article is to put forward ideas and proposals for improving the activities of internal affairs agencies related to protecting individuals, society, and the state from criminal attacks and threats of such attacks, through the comprehensive automation of working with large volumes of biometric data based on artificial intelligence and the creation of an infrastructure that meets the technological requirements.

Key words: biometric personal data, ecosystem, information technology, digital development, data economy, criminological security

Введение. Современная Россия движется по пути цивилизационного становления. Осмысление исторических предпосылок, дискуссии о категориях и понятиях, геополитические прогнозы оставим за учеными в области истории, философии, политики, сосредоточившись на факторах, касающихся темы настоящего исследования. На передний план выходят: экономическая конкурентоспособность, технологическая независимость, высокая обороноспособность, политическая, идеологическая и культурная суверенность, что в совокупности ведет к многофакторному лидерству нашей страны на международной арене, обретению внутригосударственной согласованности и стабильности развития. Однако последнее невозможно сегодня без:

– направляющей и главенствующей роли государства. «Главная особенность социальной организации в России на каждом этапе ее истории заключается в том, что государство изначально имело решающее влияние на социальную структуру и жизнедеятельность общества» [2. С. 17];

– цифровой инфраструктуры. Ее создание главным образом обеспечивалось в течение четырех предыдущих лет в рамках национальной программы «Цифровая экономика Российской Федерации», утвержденной протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7 [22];

– разработки технологий управления данными. На это направлен национальный проект «Экономика данных и цифровая трансформация государства» [23], реализация которого началась 1 января 2025 года, сменив и логически продолжив предыдущую программу. «Государство-цивилизация» должно не только обладать суверенитетом, но и занимать лидирующие позиции по стратегически определяющим направлениям, а значит задавать тенденции развития и сотрудничества вовне.

– общественного доверия. Данный пункт является одновременно и необходимым условием вышеперечисленных. В настоящее время доверие на пути цифровой трансформации обеспечивается за счет предоставления обществу, согласно теории профессора К.Х. Момджяна [9. С. 87], «объектов-медиаторов», обслуживающих надобность в поддержании качества жизни – платформы дистанционного взаимодействия между человеком, бизнесом и государством,

системы мгновенного осуществления транзакций, средства оптимицации человеческого труда за счет внедрения искусственного интеллекта и т.д. Однако, качественное и долгосрочное доверие не может быть достигнуто без удовлетворения прямой биосоциальной потребности человека, являющейся непосредственным практическим условием сохранения жизни и ее качественной составляющей - потребности в безопасности. Обеспечить эту потребность на социальном уровне призваны правоохранительные органы, средства оснащения деятельности которых должны отвечать последнему слову науки и техники. Так в рамках исполнения руководящих документов Президента и Правительства Российской Федерации по цифровой трансформации федеральных органов исполнительной власти государства в настоящий период реализуется очередная ведомственная программа цифровой трансформации (ВПЦТ) на 2025 и плановый период 2026-2027 Министерства внутренних дел Российской Федерации [21].

Основная часть. Государство, общество и личность в России не автономны по отношению друг к другу, а взаимопроницаемы, целостны, соборны [2. С. 17]. Федеральный орган исполнительной власти в лице МВД России, участвуя в программе трансформации государственного управления, обеспечивает повышение качества возложенных на него функций по:

– обеспечению безопасности государства в целом и граждан в частности;

– предоставлению государственных услуг;

– управлению государственным имуществом;

– выработке государственной политики в сфере органов внутренних дел и принятию управленческих решений.

Тем временем, одна из целей цифровой трансформации государственного управления, определенная утратившим силу распоряжением Правительства Российской Федерации от 22 октября 2021 г. № 2998-р3 «Об утверждении стратегического направления в области цифровой трансформации государственного управления», а именно обеспечение национальной безопасности и личной безопасности граждан Российской Федерации, не нашла своего отражения в актуализированном Стратегическом направлении в области цифровой трансформации государственного управления [11]. Также не находим в настоящем документе и одноименной задачи, которая прежде была утверждена. В целом же, распоряжение Правительства Российской Федерации от 16.03.2024 N 637-р не обходит стороной проблему безопасности, однако рассматривает ее применительно к критической информационной инфраструктуре и основанным на ней процессам информационного взаимодействия.

Видим важным аспектом достижения «цифровой зрелости» Министерством внутренних дел, большая часть личного состава которого приходится на подразделения, предназначенные для защиты жизни, здоровья, прав и свобод граждан

Российской Федерации, иностранных граждан, лиц без гражданства, противодействия преступности, охраны общественного порядка, собственности и обеспечения общественной безопасности [20], внедрение цифровых технологий, способствующих повышению качества вышеперечисленной деятельности органов внутренних дел. Учитывая поставленные в рамках достижения национальной цели цифровой трансформации государственного управления задачи по автоматизации модели управления на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта, а также формированию рынка данных, их активному обороту, хранению, обмену и защите, представляется целесообразным усовершенствовать применение органами внутренних дел в деятельности по защите личности, общества и государства от преступных посягательств таких персональных данных как биометрические, расширив их перечень и модернизировав систему автоматизированного учета. Эффективное использование биометрических персональных данных в обеспечении криминологической безопасности способствует оперативности изобличения лиц, причастных к совершению преступлений, и принятия процессуальных решений, а следовательно повышению эффективности деятельности правоохранительных органов по защите основ конституционного строя Российской Федерации, прав и свобод человека и гражданина, совершенствованию единой государственной системы профилактики преступности, обеспечению реализации принципа неотвратимости наказания за совершение преступления, а также формированию в обществе атмосферы нетерпимости к противоправной деятельности, что является одним из приоритетных направлений в обеспечении национальной безопасности [17].

Результаты. Из паспорта ведомственной программы цифровой трансформации МВД России на 2025 и плановый период 2026-2027 следует, что мероприятия, направленные на изменение деятельности государственного органа и переход на исполнение им государственных функций за счет использования данных в электронном виде, внедрения информационных технологий, цифровых платформ и автоматизации процессов сводятся к оказанию «государственных услуг» информационно-справочного и регистрационного характера, выполнению контрольно-надзорных функций преимущественно по обеспечению безопасности дорожного движения и миграционной политики, поддержанию информационно-телекоммуникационной инфраструктуры ведомства (табл. 1).

Таблица 1

Направления ИТ-расходов на мероприятия ВПЦТ на 2025 и плановый период 2026-2027 МВД России

Развитие и эксплуатация ведомственного сегмента ГС «Мир»[1] с целью увеличения доли предоставления следующих МСЗУ[2] в электронной форме	**Развитие информационных систем и информационно-телекоммуникационной инфраструктуры Госавтоинспекции**	**Развитие и эксплуатация информационно-телекоммуника-ционной инфраструктуры МВД России**	**Оснащение системы федерального центра обработки данных МВД России**
Смена цели въезда	Предоставление выписки о ТС в соответствии с новыми формами на ЕПГУ, в том числе об отсутствии зарегистрированных ТС	ВТКИ (внутренняя телекоммуникационная инфраструктура)	Создание и подготовка ифраструктуры ФЦОД к эксплуатации
Решение о предоставлении права на долгосрочное пребывание иностранных граждан в России			
Решение о предоставлении права на постоянное проживание иностранных граждан в России		ИРСО	
Выдача иностранным гражданам и лицам без гражданства единого документа, удостоверяющего личность иностранного гражданина на территории России, с электронным носителем информации	Автоматическое прекращение государственного учета транспортного средства	ПИРСО	
Предоставление статуса вынужденного переселенца и продление срока его действия	Возможность получения гражданином выписки о наличии у него зарегистрированных ТС или их отсутствии в режиме «онлайн» на ЕПГУ	Рабочие станции	
Оформление, выдача и замена свидетельства участника ГП по оказанию содействия добровольному переселению в РФ соотечественников, проживающих за рубежом			
Административный надзор за законностью пребывания (проживания) в России иностранных граждан	Получение информации о наличии у ФЛ и ЮЛ зарегистрированных ТС или их отсутствии в рамках КНМ в режиме «онлайн»	МВД	
Оформление и выдача паспортов гражданина РФ, удостоверяющих личность гражданина РФ за пределами территории РФ			
Функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере миграции	Контрольно-надзорная функция по осуществлению федерального государственного контроля (надзора) в области безопасности дорожного движения		

[1] ГС «Мир» - государственная система миграционного и регистрационного учета
[2] МСЗУ – массовые социально-значимые услуги

Такая структура показателей ВПЦТ призвана усовершенствовать бюрократическую составляющую деятельности органов внутренних дел, касающуюся внутреннего и внешнего документооборота, автоматизировать некоторые регистрационно-учетные функции, осуществив переход на электронное предоставление государственных услуг, ввести в эксплуатацию и развить использование государственной цифровой инфраструктуры. МВД России является многофункциональным органом исполнительной власти, но едва ли отраженные в ВПЦТ мероприятия (кроме связанных с безопасностью дорожного движения и вопросами миграции) охватывают такие наиболее важные задачи ОВД как: обеспечение защиты жизни, здоровья, прав и свобод граждан Российской Федерации, противодействие преступности, охрана общественного порядка и собственности, обеспечение общественной безопасности. На эти проблемы указывает и Н.В. Лукашов [7. С. 132], анализируя предыдущую программу цифровой трансформации МВД России на 2022–2024 годы. Согласившись с тем, что главной целью ЦТ ОВД является «приведение системы управления и организации оперативно-служебной деятельности системы МВД России в соответствие с требованиями современного информационного общества» [12. С. 36], констатируем, что на сегодняшний день большинство приоритетных направлений деятельности ОВД продолжают оставаться вне поля цифровой трансформации.

Основываясь на вышеизложенном, а также на приоритетах и целях государственной политики в сфере реализации государственной программы Российской Федерации «Обеспечение общественного порядка и противодействие преступности» [14], Положении о Министерстве внутренних дел Российской Федерации и Типовом положении о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации [18], предлагаем расширить перечень трансформируемых направлений, сфокусировав внимание на:

– предупреждении преступлений, выявлении и устранении причин и условий, способствующих их совершению;

– обеспечении безопасности граждан и правопорядка в общественных местах;

– предупреждении пресечении, раскрытии и расследовании тяжких и особо тяжких преступлений, совершенных организованными группами, преступными сообществами (преступными организациями), носящих транснациональный или межрегиональный характер, либо преступлений, вызывающих большой общественный резонанс;

– выявлении, предупреждении и пресечении экстремистской деятельности;

– противодействии терроризму, защите потенциальных объектов террористических посягательств и мест массового пребывания граждан;

– осуществлении оперативно-разыскной деятельности;

– осуществлении дознания и производстве предварительного следствия по уголовным делам;

– осуществлении экспертно-криминалистической деятельности.

Привести указанные направления деятельности ОВД в соответствие с требованиями современного информационного общества, где определяющую роль играют данные, представляется возможным путем создания биометрической экосистемы, находящейся в ведении МВД России. Сегодня подобные экосистемы находят активное применение в самых разных секторах экономики и социальной сферы, получая положительный отклик среди гражданского общества, однако, использование их в правоохранительной деятельности на постоянной основе не предусмотрено, что подтверждается в соответствующем заявлении Минцыфры [4]. В первые же годы после анонсирования и создания единой биометрической базы данных, стали выходить научные публикации, поддерживающие сбор, хранение и обработку биометрических персональных данных всех граждан России в виду того, что это позволит обеспечить высокий уровень общественной безопасности и борьбы с преступностью [16. С. 17]. Справедливости ради заметим, что порядок предоставления данных из ЕБС органам ФСБ и МВД России в целях обеспечения обороны страны и безопасности государства, охраны правопорядка, транспортной безопасности и противодействия терроризму урегулирован Правилами [13]. Однако достигнуть действительной эффективности в использовании биометрических персональных данных в правоохранительной деятельности не представляется возможным без создания ведомственного банка данных, отвечающего по своим технологическим возможностям уровню современного развития науки и техники и включающего максимальное количество биометрических характеристик, пригодных для идентификации.

Пока законодательством в рамках действия Единой биометрической системы регламентируется оборот только лишь изображения лица и записи голоса [19], люди предоставляют различным цифровым платформам отображения папиллярных узоров пальцев и ладоней, рисунка вен, радужной оболочки и сетчатки глаза, геометрии лица, руки, записи голоса, оставляют цифровые следы динамики движений при работе с клавиатурой, мышью или тачпадом. Все эти и некоторые другие биологические и физиологические параметры человека, имеющие свойства отображения на материальных носителях, а также отвечающие критериям устойчивости, универсальности и измеряемости, являются наиболее надежным и оперативным средством идентификации, то есть установления личности того или иного человека. Однако, как следует из научных трудов А.М. Зинина, реальное использование биометрических параметров для идентификации возможно тогда, когда создаются соответствующие банки данных, в которых единообразно накапливаются соответствующие образцы. «Это связано с наличием и функционированием систем регистрации человека» [3. С. 63]. Из действующих на федеральном уровне МВД России

систем регистрации биометрических персональных данных можно назвать ЦИАДИС-МВД (централизованная интегрированная автоматизированная дактилоскопическая информационная система) и ФБДГИ (федеральная база данных геномной информации) на базе сервиса объединенной поисковой федеральной системы генетической идентификации – «Ксенон-2». Таким образом из всего спектра возможностей использования биометрических персональных данных органами внутренних дел в целях обеспечения криминологической безопасности на всей территории Российской Федерации сегодня применяются: отпечатки пальцев и ладоней, а также ДНК. Другие биометрические характеристики используются фрагментарно и ситуативно, например, признаки внешности при производстве габитоскопической (портретной) экспертизы, индивидуальные признаки голоса и речи при производстве фоноскопической экспертизы, признаки почерка и подписи при производстве почерковедческой экспертизы, а также признаки внешности в совокупности с поведенческими особенностями в рамках работы с системой «Безопасный город». Идентификация посредством судебной экспертизы возможна, когда есть идентифицируемый объект (лицо в нашем случае), у которого отбираются сравнительные образцы для установления тождества с идентифицирующим объектом, изъятым в ходе осмотра места преступления или иного следственного действия (следы рук, биологические объекты, записи голоса, носители рукописного текста, фото-видеоизображения и т.д.). Однако поиску идентифицируемого лица, как правило, предшествует сложная длительная оперативно-разыскная деятельность, тогда как автоматизированный поиск по базам биометрических персональных данных не только сокращает затрачиваемое в процессе предварительного расследования время, но, как показывает практика применения ЦИАДИС-МВД, зачастую способствует раскрытию преступления «по горячим следам», в случаях с похищением человека позволяет предотвратить наступление более тяжких последствий, а при поиске без вести пропавших и вовсе предупредить возможность совершения преступления в отношении пропавшего, не говоря уже о том, что каждое своевременно раскрытое преступление являет собой предупреждение совершения новых противоправных деяний.

С трансформацией общества, переходом значительной части жизнедеятельности в цифровое пространство, меняется и криминогенная среда. Значение поисков по следам рук и ДНК никогда себя не исчерпает, но новые социально-экономические реалии формируют новые источники криминогенных рисков, а значит требуют расширения механизмов их предотвращения. В этой связи видим актуальным в рамках ведомственной программы цифровой трансформации МВД России сформулировать мероприятия, направленные на создание ведомственной биометрической экосистемы, которая будет базироваться на сборе, хранении и обработке одновременно нескольких биометрических персональных данных, например:

– фотоизображений;

– видеоизображений особенностей походки, жестикуляции и мимики;

– фонограмм речи (голоса);
– рукописных записей и подписей;
– записей клавиатурного почерка (динамики движений с устройствами ввода);
– радужной оболочки глаза;
– рисунка вен;
– геометрии руки;
– геометрии ушной раковины;
– папиллярных узоров рук;
– ДНК;
– термограмм;
– других вновь выявляемых для идентификации данных, как например электрокардиограмм [8].

Кроме баз данных, элементами экосистемы могут стать портативные мультимодальные сканеры, обеспечивающие ввод и обработку расширенного количества биометрических персональных данных: геометрия лица, руки, запись голоса(речи), рисунок вен, термограмма, радужная оболочка глаза, отпечатки пальцев и ладоней.

В перспективе, когда биометрические персональные данные перестанут быть предметом социального напряжения, вызывая в обществе тревогу и опасения, как и все когда-то новое Д.Н. Баринов пишет: «в ходе социализации в рамках новых для индивида форм совместной деятельности…появляются страхи, связанные с новыми взаимоотношениями, социальными ролями и статусами, нормами и правилами» [1. С. 44], видим возможность оснащения биометрическими сканерами нового поколения мест большого скопления или потока людей для предупреждения и пресечения преступлений. Так, например, лента поручня эскалатора может быть оснащена сканером, считывающим геометрию руки, рисунка вен или папиллярных узоров пальцев и ладоней, с целью своевременного обнаружения лиц, находящихся в уголовном розыске или числящихся без вести пропавшими. Сотрудники оперативных подразделений и патрульно-постовой службы МВД России могут быть снабжены специальными техническими средствами в виде очков биометрического видения, которые по геометрии лица, мимике, жестикуляции, походке помогут в выявлении лиц, представляющих оперативный интерес. Такие средства, например, смогут использоваться вне больших городов, оснащенных камерами видеонаблюдения с системой распознавания лиц.

Особое внимание при создании соответствующей цифровой инфраструктуры считаем целесообразным уделить применению алгоритмов искусственного интеллекта, потому как опыт внедрения версии АДИС Папилон-9 и ПО «НейроЭксперт» в МВД России по Республике Крым, где в обработке дактилоскопических данных задействованы нейросети, продемонстрировал возможность 40-кратного сокращения трудозатрат эксперта в процессе идентификации и увеличение результативности на

3,7 % [10] без потери качества. Принятие же окончательного решения по результатам автоматизированной обработки целесообразно оставить за человеком (уполномоченным сотрудником), к чему приходят и зарубежные исследователи в анализе использования по всему миру автоматизированных систем распознавания лиц, рекомендуя полицейским полагаться на искусственный интеллект для составления списков кандидатов, а затем проводить субъективные сравнения таким образом, чтобы получить приемлемые заключения [15]. Представляется, что наделение искусственного интеллекта большими или меньшими полномочиями в обработке биометрических персональных данных зависит от достаточности и достоверности комплекса индивидуальных признаков, что при апробировании внедряемых в деятельность МВД России биометрических технологий может быть предоставлено на оценку криминалистов. В целом же, научным сообществом давно замечено, что использование технологий, функционирующих на основе искусственного интеллекта, который способствует быстрому собиранию, отслеживанию и анализу различных информационных потоков и данных с целью противодействия преступным проявлениям, является чрезвычайно эффективным [6. С. 109].

Заключение. Создание предлагаемой биометрической экосистемы в рамках достижения национальной цели цифровой трансформации государственного управления позволит МВД России выйти на новый уровень в обеспечении криминологической безопасности, продемонстрировав выполнение задач по автоматизации модели управления и оперативно-служебной деятельности на основе данных с учетом ускоренного внедрения технологий обработки больших объемов информации, машинного обучения и искусственного интеллекта, а также расширению ведомственного банка биометрических данных, их активному использованию, хранению и защите.

Положительный эффект от применения органами внутренних дел комплекса цифровых платформ хранения и автоматизированной с помощью искусственного интеллекта обработки биометрических персональных данных в условиях современного информационного общества представляется в удовлетворении следующих основных целей обеспечения криминологической безопасности:

– оптимизация деятельности ОВД, направленной на минимизацию криминогенного потенциала источников угроз криминологической безопасности;

– активизация предупредительного потенциала деятельности ОВД;

– минимизация уязвимости личности, общества, государства перед криминогенными рисками;

– формирование у населения ощущения состояния защищенности от преступных посягательств и угроз таких посягательств.

Кроме того, комплексное внедрение цифровой инфраструктуры и искусственного интеллекта в непосредственно оперативно-служебную деятельность наравне с усовершенствованием навыков сотрудников ОВД по использованию новых

технологий призвано не только улучшить показатели в работе, повысить уровень общественного доверия, но и поднять престиж службы, обеспечив приток молодых кадров. Как справедливо замечает П.Н. Кобец «немаловажно стремиться к тому, чтобы инновационные технологии не внедрялись с большими опозданиями, а в целом инновационная деятельность в МВД России соответствовала бы общемировым тенденциям и динамике» [5. С. 167].

Список литературы

1. Баринов Д.Н. Страх как социальный феномен // Гуманитарный научный вестник. 2019. №2. С. 39-48.

2. Зарубина Е. В, Журавлева Л. А., Ларин М. В., Симачкова Н. Н., Чупина И. П. Россия как государство-цивилизация // Образование и право. 2024. №11. С. 13-19.

3. Зинин А. М. Идентификация человека по признакам внешности и методы биометрии // Вестник Университета имени О. Е. Кутафина. 2022. №2 (90). URL: https://cyberleninka.ru/article/n/identifikatsiya-cheloveka-po-priznakam-vneshnosti-i-metody-biometrii (дата обращения: 02.09.2025).

4. Информация Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15 мая 2024 г. "Единую биометрическую систему нельзя использовать для розыска людей" Электронный ресурс. - Режим доступа: URL: https://base.garant.ru/409019488/ (дата обращения: 01.09.2025)

5. Кобец П.Н. Внедрение технологий, использующих искусственный интеллект, в деятельность МВД России: опыт и проблемы // Вестник ВИПК МВД России. 2023. No 4(68). С. 161-168; doi: 10.29039/2312-7937-2023-4-161-16.

6. Кравцов Д.А. Искусственный разум: предупреждение и прогнозирование преступности // Вестник Московского университета МВД России. 2018. No 3. С. 108-111.

7. Лукашов Николай Васильевич. Теоретические и организационные основы цифровой трансформации территориальных органов внутренних дел системы МВД России // Труды Академии управления МВД России. 2023. № 3 (67). С. 128-137.

8. Meltzer D, Luengo D. ECG-Based Biometric Recognition: A Survey of Methods and Databases. Sensors (Basel). 2025;25(6):1864. Published 2025 Mar 17. doi:10.3390/s25061864

9. Момджян К. Х. К типологии человеческих потребностей. Статья 2. Биосоциальная потребность в безопасности // Вестник Московского университета. Серия 7: Философия. 2015. № 5. С. 77-90.

10. Нейросетевой анализ рекомендательных списков в АДИС ПАПИЛОН-9: Миас, Москва - март 2023. // Электронный ресурс URL: https://docs.yandex.ru/docs/view?tm=1757542983&tld=ru&lang=ru&name=АДИС_Нейро_08_05.pdf (дата обращения 02.09.2025).

11. Об утверждении стратегического направления в области цифровой трансформации государственного управления : распоряжение Правительства Рос. Федерации от 16.03.2024 N 637-р // СПС КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_472443/929117c006b16895e2e322b7cf9bb78632871730/ (дата обращения: 27.08.2025)

12. Отчет о научно-исследовательской работе «Проект концепции цифровой трансформации системы МВД России» (заключительный), заявка ДИТСиЗИ МВД России от 15 фев. 2022 г. № 9/1285, рег. № НИОКТР 01221755. Москва: Академия управления МВД России, 2022.

13. Постановление Правительства РФ от 28 декабря 2018 г. N 1703 «О предоставлении оператором единой биометрической системы и оператором регионального сегмента единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической системе и региональном сегменте единой биометрической системы» (с изменениями и дополнениями) // Электронный ресурс – URL: https://base.garant.ru/72141570/ (дата обращения 02.09.2025)

14. Постановление Правительства РФ от 15.04.2014 N 345 (ред. от 31.08.2024) «Об утверждении государственной программы Российской Федерации «Обеспечение общественного порядка и противодействие преступности» // СПС КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_162172/9553e2de22c93e2264458e072038297f1c534662/ (дата обращения: 01.09.2025)

15. Ritchie KL, Cartledge C, Growns B, et al. Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. PLoS One. 2021;16(10):e0258241. Published 2021 Oct 13. doi:10.1371/journal.pone.0258241

16. Степенко В. Е., Богдановская А. Д. Биометрические персональные данные // Евразийский союз ученых. 2020. № 4-10(73). С. 15-19.

17. Указ Президента РФ от 02.07.2021 N 400 "О Стратегии национальной безопасности Российской Федерации" // СПС КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 01.09.2025)

18. Указ Президента РФ от 21.12.2016 N 699 (ред. от 15.05.2025) «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации» // СПС КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_209309/ (дата обращения: 01.09.2025)

19. Федеральный закон "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных

данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" от 29.12.2022 N 572-ФЗ (последняя редакция) // СПС КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_436110/ (дата обращения: 01.09.2025).

20. Федеральный закон от 07.02.2011 N 3-ФЗ (ред. от 31.07.2025) «О полиции» (с изм. и доп., вступ. в силу с 01.09.2025), ст.1.

21. Электронный ресурс. - Режим доступа: URL: https://gis.gov.ru/documents (дата обращения 27.08.2025).

22. Электронный ресурс. – Режим доступа: URL: https://digital.gov.ru/target/naczionalnaya-programma-czifrovaya-ekonomika-rossijskoj-federaczii (дата обращения 27.08.2025).

23. Электронный ресурс. – Режим доступа: URL: https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva (дата обращения 27.08.2025).

УДК 34:004.056

Ю. М. Билялова,
начальник учебного отдела,
Казанский юридический институт (филиал)
ФГКОУ ВО «Университет прокуратуры
Российской Федерации»

Роль искусственного интеллекта в борьбе с киберпреступностью: возможности и ограничения

Аннотация. В статье рассматриваются возможности и ограничения применения искусственного интеллекта в сфере кибербезопасности. Анализируются современные методы обнаружения и предотвращения кибератак с использованием машинного обучения и нейросетевых моделей, а также вопросы прогнозирования угроз. Особое внимание уделяется техническим, этическим и правовым вызовам, связанным с внедрением ИИ-технологий. Сделан вывод о необходимости комплексного подхода для эффективной защиты информационных систем в условиях быстро меняющегося киберпространства.

Ключевые слова: искусственный интеллект, кибербезопасность, машинное обучение, кибератаки, нейросети, автоматизация, этика, правовые аспекты, информационная безопасность, прогнозирование угроз

Y. M. Biliyalova
Head of the Training Department,
Kazan Law Institute (branch) of the Federal State Establishment of Higher Education
«University of the Prosecutor office of the Russian Federation»

The role of artificial intelligence in combating cybercrime: opportunities and limitations

Abstract. The article discusses the possibilities and limitations of using artificial intelligence in the field of cybersecurity. It analyzes modern methods of detecting and preventing cyberattacks using machine learning and neural network models, as well as the issues of threat forecasting. Special attention is paid to the technical, ethical, and legal challenges associated with the implementation of AI technologies. The article concludes that a comprehensive approach is necessary for effective protection of information systems in a rapidly changing cyberspace.

Keywords: artificial intelligence, cybersecurity, machine learning, cyberattacks, neural networks, automation, ethics, legal aspects, information security, threat forecasting

Введение. В условиях стремительного развития цифровых технологий киберпреступность становится одной из ключевых угроз информационной

безопасности, подобно зловещей тени, неустанно преследующей цифровой мир и становящейся все более изощренной и разрушительной. С каждым днем появляются новые вирусы, фишинговые атаки становятся все более правдоподобными, а киберпреступники используют уязвимости в сложных системах для кражи данных, вывода из строя критически важной инфраструктуры и получения финансовой выгоды. Традиционные методы защиты часто оказываются недостаточно эффективными против современных сложных атак. В этой бесконечной гонке за преимуществом искусственный интеллект предлагает новые возможности для обнаружения, анализа и предотвращения кибератак, повышая уровень защиты информационных систем [1]. Вместе с тем, внедрение искусственного интеллекта связано с рядом технических, этических и правовых вызовов [6], но его возможности не безграничны.

Основная часть. Искусственный интеллект можно использовать как щит и меч от киберугроз. В связи с этим целесообразно изучить новые возможности, которые искусственный интеллект предоставляет для противодействия киберпреступности.

Системы искусственного интеллекта в отличии от человека способны обрабатывать и анализировать большие объемы информации, выявлять отклонения и подозрительные модели поведения, что может свидетельствовать о возможных кибератаках [4]. Методы машинного обучения и нейронные сети в настоящее время эффективно используются для обнаружения новых типов вредоносного программного обеспечения и первоначальных атак, типа «нулевой день» [11]. Автоматизированный процесс реагирования на случаи с применением искусственного интеллекта ускоряет процесс ответа и может уменьшить потенциальный вред [10].

В настоящее время в эпоху цифровой трансформации защита информации является стратегически важным аспектом. Для обеспечения безопасности в информационной среде все чаще используется различные техники искусственного интеллекта и машинного обучения: от обнаружения аномалий до предотвращения угроз. А системы, основанные на искусственном интеллекте, обладают огромным выбором технологических методов для противодействия киберугрозам. Они превосходят привычные традиционные методы, основанные на анализе эталонных моделей и ручном реагировании. Таким образом можно выявить следующие основные виды применения искусственного интеллекта в условиях кибербезопасности.

В режиме реального времени искусственный интеллект отражает киберугрозы, обнаруживает те или иные ошибки и аномалии. Для обнаружения различных угроз искусственный интеллект осуществляет мониторинг сетевого трафика, проводит анализ журналов событий и также способен отслеживать поведение пользователей. Все перечисленные действия могут заранее указать на наличие отклонений или внутренних угроз. А с помощью машинного обучения системы искусственного интеллекта способны адаптироваться к новым атакам и постоянно совершенствуют свою работу [2].

Также, искусственный интеллект способен реагировать на действия в автоматическом режиме. После обнаружения угрозы он фильтрует поступающую информацию и нейтрализует угрозу, в том числе без участия человека. Данные действия позволяют сотрудникам по информационной безопасности вовремя принять меры для устранения или снижения возможных атак, что ускоряет процесс реагирования на кибератаки и снижает ущерб от них [1].

Банковская система в России активно внедряет искусственный интеллект для борьбы с мошенниками, который анализирует информацию из разных источников, таких как текст, голос и изображения для выявления подозрительных транзакций, поддельных документов и признаков социальной инженерии, тем самым предупреждая пользователей о возможных попытках обмана.

В целом аналитические модели, разработанные на основе искусственного интеллекта, помогают спрогнозировать возможные кибератаки, анализировать полученные данные и выявлять слабые места в инфраструктуре [10]. Это позволяет организациям предпринимать действенные меры по усилению защиты и обнаруживать за короткие сроки аномалии, которые указывают на киберугрозу, еще до того, как произошла атака.

Несмотря на огромный потенциал, использование искусственного интеллекта в сфере кибербезопасности имеет свои риски и порождает новые проблемы. Эффективность искусственного интеллекта напрямую зависит от качества и объема применяемых данных. Недостаток или искажение данных может привести к ошибочным заключениям и ложным срабатываниям, что снижает доверие к этим системам [7].

Рассмотрим некоторые ограничения искусственного интеллекта:

– так называемая борьба «искусственный интеллект против искусственного интеллекта». Киберпреступники также используют искусственный интеллект для разработки более изощренных видов преступлений, корректируют стратегию атаки на защитные механизмы организаций и автоматизации вредоносной деятельности. Это приводит к непрерывной гонке вооружений, в которой обе стороны постоянно совершенствуют свои технологии [8, 10].

– технологии машинного обучения часто функционируют как «черный ящик», что затрудняет понимание как искусственный интеллект обрабатывает данные и принимает те или иные решения. Это ставит вопрос: можно ли доверять системе, у которой отсутствует логическая цепочка принятия решения.

– автоматизированный процесс безопасности при помощи искусственного интеллекта ставит определенные вопросы конфиденциальности, ответственности и прозрачности принимаемых решений. Машинное обучение способно выдавать ошибки ввиду неполных или неактуальных данных. Законодательство России и других стран постепенно адаптируется к этим вызовам, однако многие вопросы остаются нерешенными [5].

Не смотря на трудности и возникающие проблемы кибербезопасность под влиянием искусственного интеллекта переживает настоящую трансформацию во всех сферах деятельности, при этом обещая революционные прорывы в защите данных. Однако, критическая оценка возможностей и рисков, которые несет в себе искусственный интеллект, требует тщательного анализа. В условиях цифровой трансформации и стремительного развития технологий в государственной политике Российской Федерации в направлении развития искусственного интеллекта и кибербезопасности эти вопросы приобретают особую актуальность [9].

При этом искусственный интеллект становится незаменимым помощником по защите от киберпреступлений. Но чтобы искусственный интеллект раскрыл весь свой потенциал, необходимо проделать большую работу. Ключевым аспектом для достижения этой цели является совместная работа представителей кибербезопасности и не только их, поскольку будущее кибербезопасности невозможно представить без тесного взаимодействия. Только объединив силы государства, науки и бизнеса, мы сможем максимально эффективно использовать весь арсенал лучших практик и знаний по искусственному интллекту. Обмен опытом, особенно в таких критически важных сферах, как искусственный интеллект и кибербезопасность, позволит нам не просто идти в ногу со временем, но и опережать современные угрозы, ускоряя наш общий прогресс в этой жизненно важной области.

Кроме того, нельзя недооценивать роль человека. Подготовка высококвалифицированных специалистов, которые смогут создавать, внедрять и поддерживать технологии искусственного интеллекта – это залог нашего успеха. Профессионал в области кибербезопасности должен соответствовать современным реалиям и быть в курсе постоянных инноваций. Тем более, принимая во внимания скорость развития искусственного интеллекта, профессии, касающиеся обработки информации и аналитики, становятся более востребованными.

Заключение. Подводя итог можно сделать следующий вывод. Искусственный интеллект и машинное обучение формируют будущее кибербезопасности, улучшая обнаружение угроз и автоматизируя реагирование.

Он не только помогает быстрее находить риски и самые изощренные угрозы, но и делает этот процесс точнее, а реагирование на кибератаки – куда эффективнее [12. С. 121-122]. Однако, чтобы в полной мере воспользоваться всеми преимуществами искусственного интеллекта, мы должны помнить о его проблемах, следовать этическим правилам и учитывать правовое законодательство.

Список литературы

1. Банкетов Д.А., Федоров М.А., Пальмов С.В. Роль искусственного интеллекта в кибербезопасности // Индустриальная экономика. 2024. №S1. URL: https://cyberleninka.ru/article/n/rol-iskusstvennogo-intellekta-v-kiberbezopasnosti-1.

2. Бекматов А. К., Кутдусова Э. Р., Мукимов Ш. И., Давлатова Н. Н. Прогрессивные тенденции применения искусственного интеллекта в области информационной безопасности // Экономика и социум. 2023. №6-1 (109). URL: https://cyberleninka.ru/article/n/progressivnye-tendentsii-primeneniya-iskusstvennogo-intellekta-v-oblasti-informatsionnoy-bezopasnosti.

3. Дубровина А. И. Гибридный метод моделирования систем искусственного интеллекта для выявления кибератак // Вестник ДГТУ. Технические науки. 2025. №2. URL: https://cyberleninka.ru/article/n/gibridnyy-metod-modelirovaniya-sistem-iskusstvennogo-intellekta-dlya-vyyavleniya-kiberatak.

4. Задбоев В.А., Робак В.А., Мелехов К.В. Модель средства контроля сети передачи данных для выявления аномалий, раннего обнаружения и классификации атак // Теория и практика обеспечения информационной безопасности: сборник трудов III Всероссийской научно-практической конференции, Москва, 08 ноября 2023 года. 2023. С. 42-49.

5. Козлова Н.Ш., Довгаль В.А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2023. №3 (326). URL: https://cyberleninka.ru/article/n/analiz-primeneniya-iskusstvennogo-intellekta-i-mashinnogo-obucheniya-v-kiberbezopasnosti.

6. Лобачева А.С., Соболь О.В. Этика применения искусственного интеллекта в управлении персоналом // E-Management. 2021. №1. URL: https://cyberleninka.ru/article/n/etika-primeneniya-iskusstvennogo-intellekta-v-upravlenii-personalom.

7. Лощилин А.В., Яриков В.Г., Никишова А.В. Методы машинного обучения в прогнозировании и предотвращении кибератак // NBI-technologies. 2024. №2. URL: https://cyberleninka.ru/article/n/metody-mashinnogo-obucheniya-v-prognozirovanii-i-predotvraschenii-kiberatak.

8. Намиот Д. Е. О кибератаках с помощью систем Искусственного интеллекта // International Journal of Open Information Technologies. 2024. №9. URL: https://cyberleninka.ru/article/n/o-kiberatakah-s-pomoschyu-sistem-iskusstvennogo-intellekta.

9. Репин Д.А. Технологии искусственного интеллекта как фактор совершенствования государственного управления: вызовы и угрозы // Экономика и управление. 2025. №2. URL: https://cyberleninka.ru/article/n/tehnologii-iskusstvennogo-intellekta-kak-faktor-sovershenstvovaniya-gosudarstvennogo-upravleniya-vyzovy-i-ugrozy.

10. Самолкаева А. М., Шведова С. М. Искусственный интеллект в сфере информационной безопасности: преимущества, ограничения и перспективы // Вестник науки. 2024. №3 (72). URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-sfere-informatsionnoy-bezopasnosti-preimuschestva-ogranicheniya-i-perspektivy.

11. Хакимов А.А. Роль искусственного интеллекта в кибербезопасности // Universum: технические науки. 2023. №11-1 (116). URL: https://cyberleninka.ru/article/n/rol-iskusstvennogo-intellekta-v-kiberbezopasnosti.

12. 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.

УДК 343.2/.7

Д. А. Бородин,
аспирант,
Университет прокуратуры Российской Федерации,
Санкт-Петербургский юридический институт (филиал)

Использование информационных систем в целях противодействия совершению преступлений в сфере публичных закупок: опыт прокурорского надзора

Аннотация. В статье приводится опыт использования российских информационных систем и интернет-сервисов, применяемых при осуществлении прокурорского надзора за исполнением федерального законодательства в сфере публичных закупок. Рассматриваются примеры эффективного использования цифровых технологий при осуществлении прокурорского надзора, позволившего минимизировать ущерб от совершенных противоправных действий в отношении бюджетных денежных средств. Делается вывод о важности применения официальных информационных систем и интернет-сервисов при реализации полномочий прокурора в сфере закупок, в том числе в целях минимизации ущерба от противоправной деятельности.

Ключевые слова: цифровые технологии, информационные системы, интернет-сервис, прокурорский надзор, публичные закупки, государственные закупки, ущерб от совершения преступления

D. A. Borodin,
postgraduate student,
University of the Prosecutor's Office of the Russian Federation,
St. Petersburg Law Institute (branch)

The use of information systems to counteract the commission of crimes in the field of public procurement: the experience of prosecutorial supervision

Abstract. The article presents the experience of using Russian information systems and Internet services used in the implementation of prosecutorial supervision of the implementation of federal legislation in the field of public procurement. The article considers examples of the effective use of digital technologies in the implementation of prosecutorial supervision, which made it possible to minimize damage from illegal actions committed in relation to budgetary funds. The conclusion is made about the importance of using official information systems and Internet services in the exercise of the prosecutor's powers in the field of procurement., in particular, in order to minimize damage from illegal activities.

Keywords: digital technologies, information systems, Internet service, prosecutor's supervision, public procurement, public procurement, damage caused by the commission of a crime

Введение. Совершение преступлений в сфере публичных закупок является одной из наиболее актуальных проблем российского общества. И причиной тому не только большой резонанс уголовных дел, получаемых огласку в СМИ, в которых предметом преступлений выступают порою миллиарды рублей из государственных и муниципальных бюджетов [1].

Обеспокоенность вызывает и то, что преступления в сфере закупок приобрели всеобъемлющий характер: они совершаются в каждом субъекте Российской Федерации, а их субъектами выступают представители публичной власти почти любого уровня, начиная, от глав небольших муниципальных образований, заканчивая, губернаторами и заместителями федеральных министров [2, 3, 10].

Именно поэтому обеспечение законности в сфере закупок является одним из наиболее приоритетных направлений деятельности органов прокуратуры, что подчеркнуто требованием Генерального прокурора Российской Федерации к подчиненным прокурорам «принять дополнительные меры по укреплению законности и координации борьбы с преступностью в сфере закупок» [9].

Основная часть. Практика использования информационных систем и интернет-сервисов в целях противодействия совершению преступлений в сфере закупок. С момента своего появления в современном российском государстве сфера публичных закупок претерпела существенные изменения. Сегодня процедура закупок проводится с использованием цифровых технологий в единой информационной системе (ЕИС), и надзорно-контрольные органы получили беспрецедентные возможности эффективно реализовывать свои полномочия, дистанционно контролируя процедуры закупок без необходимости проведения выездной проверки по каждой из них.

Тем не менее проведение закупок в ЕИС одномоментно не лишило возможности участников преступных схем присваивать бюджетные денежные средства и совершать иные преступления в указанной сфере, что обусловлено рядом факторов. Одним из таких факторов является проблема использования «больших данных». Ежедневно количество совершаемых закупок исчисляется тысячами, а объем информации и документации о тех из них, которые проводятся поднадзорными (подконтрольными) объектами на уровне конкретного подразделения контрольно-надзорного органа, невероятно высок.

В этих условиях очевидна необходимость использования цифровых технологий и информационных систем, позволяющих анализировать большие объемы данных и получать необходимую информацию в считанные минуты, анализ которой работником компетентного органа занял бы часы или дни.

Так, в органах прокуратуры при проведении надзорных мероприятий в сфере закупок на постоянной основе обеспечено использование следующих информационных систем:

1. Система межведомственного электронного взаимодействия (СМЭВ) позволяет получать актуальную информацию об объектах проверки, их должностных лицах путем направления электронных запросов к банкам данных иных органов государственной власти: МВД, ФНС, Росреестра, Федерального казначейства и т.д. [7]. В отличие от существовавшей ранее необходимости направления письменных запросов в указанные органы, ответы на которые, порою поступали спустя дни или недели, результаты большого количества запросов в СМЭВ приходят в считанные минуты.

Использование СМЭВ крайне эффективно при выявлении признаков аффилированности уполномоченного лица, представляющего интересы заказчика в сфере закупок, с поставщиком по контракту, например, с помощью данной системы имеется возможность выявить факт участия близкого родственника уполномоченного лица в уставном капитале коммерческой организации, исполняющей контракт.

2. Информационная система «СПАРК» является агрегатором общедоступной информации, а также информации из официальных источников о юридических лицах и индивидуальных предпринимателях, с помощью которого органы прокуратуры получают сведения об регистрационных данных организаций, их участии в судах, возбужденных в отношении них исполнительных производств и т.д. [5].

Одними из наиболее полезных функций данной системы в контексте проведения надзорных мероприятий являются разделы «Анализ владения», отражающий текущие сведения об участниках в уставном капитале организации, и «Связи компании», где представлены сведения о составе тех органов управления и контроля, акционерах и контролирующих лицах, которые участвуют в уставном капитале одновременно и в проверяемой, и в иных организациях. Не менее важным является раздел «Регистрационные данные, Изменения», в котором хронологически отражены сведения, к примеру, об изменении состава участников и их долей в уставном капитале.

3. Информационная система «Маркер» используется для мониторинга, анализа и контроля процедуры закупок [4]. Системой проводится анализ конкретной закупки, результатом которого является выделение различных индикаторов риска: от нарушения установленных сроков заключения и исполнения контракта (как со стороны заказчика, так и со стороны поставщика), нахождения поставщика в реестре недобросовестных поставщиков до признаков завышения цены контракта или наличия картельного сговора.

Указанные информационные системы являются важным подспорьем при проведении прокурорских проверок в сфере закупок, однако прокурорам не стоит ограничиваться лишь ими. Информация, необходимая для пресечения преступлений в указанной сфере и минимизации ущерба от их совершения, далеко не всегда

находится в банках данных органов государственной власти, что подтверждается практикой прокурорской деятельности.

Так, Приморской межрайонной прокуратурой Архангельской области при надзорном сопровождения исполнения государственного контракта по объекту «Строительство здания участковой больницы на 40 посещений и стационаром на 10 коек в поселке Соловецкий» ценой в 638,1 млн. руб. установлено, что учредителем ООО «Белый дом» Н. (поставщик) от и.о. руководителя ГКУ АО «Главное управление капитального строительства» (заказчик) 19.03.2021 получено согласование на приобретение не предусмотренной контрактом аэролодки «Север 750К» стоимостью 9,9 млн. руб.

Покупка аэролодки обосновывалась тем, что она будет использоваться для доставки рабочих и стройматериалов в пос. Соловецкий, располагающийся на одноименном архипелаге. Вместе с тем водное транспортное средство по своим техническим характеристикам было неспособно обеспечить исполнение контракта в части перевозки грузов и пассажиров в акватории Белого моря.

Впоследствии решением нового и.о. ГКУ АО «ГУКС» от 09.09.2023 в связи с нарушением поставщиком сроков исполнения работ заказчиком принято решение о расторжении государственного контракта в одностороннем порядке. Поставщиком в Арбитражный суд Архангельской области направлено исковое заявление о признании данного решения незаконным (дело № А05-8006/2023).

Однако в связи с расторжением контракта учредителем коммерческой организации Н. были предприняты попытки сокрытия имущества организации (в том числе аэролодки), которое могло бы быть обращено в пользу заказчика, в рамках рассмотрения других арбитражных дел о взыскании ущерба, неосновательного обогащения в пользу заказчика, а также банкротства коммерческой организации, так и конфисковано приговором суда в рамках уголовного дела, которое могло быть возбуждено в связи с нарушениями, допущенными Н. при исполнении контракта.

Подготовка к сокрытию имущества и факты этого выявлены межрайонной прокуратурой с помощью использования не только информационных систем, но и общедоступных интернет-сервисов. Так, с использованием данных информационной системы «СПАРК» выявлены изменения в регистрационных данных компании, а именно с 17.04.2023 в налоговом органе зарегистрировано назначение С. на должность нового генерального директора общества, который имел признаки «номинального» руководителя.

Также было обнаружено, что в интернет-сервисе «Авито» (Avito.ru) 13.03.2024 размещено объявление о продаже аэролодки с характеристиками, соответствующими приобретенной ранее заказчиком в рамках исполнения государственного контракта. При этом продавцом указана К., что позволяет идентифицировать ее с генеральным директором ООО «Белый дом» С., имевшей девичью фамилию К., а местонахождение

продавца в объявлении совпадает с местом регистрации и фактического нахождения общества.

В целях пресечения сокрытия имущества межрайонной прокуратурой в рамках рассмотрения вышеуказанного арбитражного дела заявлено ходатайство о принятии обеспечительных мер в виде наложения ареста на маломерное судно, которое определением от 15.03.2024 удовлетворено [6].

Позднее в рамках производства по уголовному делу в отношении учредителя организации Н. по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ, на водное транспортное средство вновь был наложен арест, а судьба транспортного средства разрешена при постановлении приговора [8].

Заключение. Таким образом, комплексное использование достижений развития цифровых технологий – официальных информационных систем, а также общедоступных интернет-сервисов позволяет в полной мере реализовывать надзорные полномочия органов прокуратуры в целях противодействия совершения преступлений в сфере публичных закупок.

Как показывает опыт прокурорской деятельности использование информационных систем и сервисов важно не только для привлечения виновных лиц к установленной законом ответственности по факту совершения преступлений, но и для минимизации имущественного ущерба, который они причиняют его совершением, и в конечном итоге – возвращения в государственный (муниципальный) бюджет денежных средств.

В условиях современного уровня развития технологий использование информационных систем и сервисов должно осуществляться при проведении каждого надзорного мероприятия в сфере закупок, а также при расследовании уголовных дел.

Список литературы

1. «Аресты генералов» // Сайт газеты «РБК» [Электронный ресурс]. URL: https://www.rbc.ru/story/66c6fc4b9a7947b932ee34c3 (дата обращения: 03.09.2025).

2. «Дело Тимура Иванова: как и за что задержали замминистра обороны» // Сайт газеты «РБК» [Электронный ресурс]. URL: https://www.rbc.ru/society/24/04/2024/6628b20f9a79476478006945 (дата обращения: 04.09.2025).

3. «Глава томского поселения получил срок за растрату бюджетных средств» // Сайт газеты «Комсомольская правда» [Электронный ресурс]. URL: https://www.tomsk.kp.ru/online/news/6539753 (дата обращения: 03.09.2025).

4. Информационный ресурс «Маркер» // Сайт АО «Интерфакс» [Электронный ресурс]. URL: https://marker-interfax.ru (дата обращения: 04.09.2025).

5. Информационный ресурс «СПАРК» // Сайт АО «Информационное агентство «Интерфакс» [Электронный ресурс]. URL: https://spark-interfax.ru (дата обращения: 04.09.2025).

6. Определение Арбитражного суда Архангельской области от 15 марта 2024 года по делу № А05-8006/2023 // Доступ из «Картотека арбитражных дел» [Электронный ресурс]. URL: https://kad.arbitr.ru/Document/Pdf/56452824-19be-4a7f-a067-4c3f8d2b3e2e/30a249e8-7184-41f9-bcdd-039cea9bbf02/A05-8006-2023_20240315_Opredelenie.pdf?isAddStamp=True (дата обращения: 04.09.2025).

7. Постановление Правительства Российской Федерации от 08.09.2010 № 697 (ред. от 28.11.2024) «О единой системе межведомственного электронного взаимодействия» // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_491831 (дата обращения: 04.09.2025).

8. Приговор Октябрьского районного суда г. Архангельска от 12 мая 2025 года по делу № 1-73/2025 // Доступ из ГАС «Правосудие» [Электронный ресурс]. URL: https://oktsud--arh.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=249317142&case_uid=e080e1eb-d69c-47a4-87d6-6d42b0ea9bf1&delo_id=1540006 (дата обращения: 04.09.2025).

9. Приказ Генерального прокурора Российской Федерации от 14.01.2021 (ред. от 05.05.2023) № 6 «Об организации прокурорского надзора за исполнением законодательства в сфере закупок» // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_374322 (дата обращения: 04.09.2025).

10. «Рязань посадочная. Экс-губернатора арестовали вслед за его заместителем и сенатором» // Сайт газеты «Коммерсантъ» [Электронный ресурс]. URL: https://www.kommersant.ru/doc/7365975 (дата обращения: 03.09.2025).

УДК 343.131

Р. С. Бурганов,
кандидат юридических наук, доцент,
Казанский филиал Российского государственного университета правосудия
имени В.М. Лебедева

Значение электронного уголовного дела для предупреждения преступных правонарушений должностных лиц уголовного судопроизводства

Аннотация: Статья посвящена влиянию технологий электронного уголовного дела на предупреждение преступных правонарушений должностных лиц уголовного судопроизводства. Ведение уголовного дела в электронном виде сделает невозможным или, по крайней мере, существенно усложнит фальсификацию материалов уголовного дела, воспрепятствование осуществлению правосудия и предварительного расследования при осуществлении производства по уголовному делу. Фиксирование всех процессуальных действий и процессуальных решений на специальной платформе позволит отследить те изменения, которые вносились в материалы уголовного дела, предоставить необходимые полномочия пользователям, установить хронологию внесения изменений и работы с платформой. Рассматриваемые изменения позволят существенно оптимизировать и сделать более эффективной работу органов дознания, следственных, прокурорских и судебных органов.

Ключевые слова: сотрудник правоохранительных органов, судебные органы, должностное лицо, электронное уголовное дело, предупреждение преступлений, фальсификация доказательств

R.S. Burganov,
Candidate of Law, Associate Professor
Criminal Law Disciplines of the Kazan branch of the Russian State University of
Justice named after V.M. Lebedev

The importance of electronic criminal cases for preventing criminal violations by criminal prosecution officials

Abstract. The article is devoted to the impact of electronic criminal case technologies on preventing criminal violations by criminal prosecuting officials. Conducting a criminal case electronically will make it impossible or, at least, significantly more difficult to falsify criminal case materials, obstruct the administration of justice and preliminary investigation during criminal proceedings. Recording all procedural actions and procedural decisions on a special platform will allow tracking the changes made to the criminal case materials, granting the necessary powers to users, establishing the chronology of changes and work with the platform. The changes under consideration will significantly optimize and make the work of inquiry, investigative, prosecutorial and judicial bodies more efficient.

Keywords: law enforcement officer, judicial bodies, official, electronic criminal case, crime prevention, falsification of evidence.

Введение. Развитие уголовного судопроизводства на основе информатизации и цифровизации должно неизбежно реализоваться в создании электронного уголовного дела. Его материальной основой должна стать единая платформа электронного уголовного судопроизводства.

Основная часть. На данной платформе смогут осуществлять свои уголовно-процессуальные права, обязанности и полномочия самые разные должностные и недолжностные лица, органы, которые являются участниками уголовного судопроизводства. К этим лицам можно отнести:

– правоохранительные органы, отдельные их подразделения, обладающие уголовно-процессуальным статусом. Например, отдел полиции, прокуратура района, управление Следственного комитета РФ и т.д.;

– отдельные должностные лица уголовного судопроизводства (следователь, дознаватель, судья, прокурор и др.);

– лица, не являющиеся должностными, но участвующие в уголовном судопроизводстве (подозреваемый, обвиняемый, потерпевший и др.).

На необходимость создания указанной платформы неоднократно указывалось в правовой науке. Так,

М.А. Гаврилов пишет: «…можно констатировать главное - для обеспечения реализации положений закона назрела необходимость использования в рамках уголовного судопроизводства единой электронной системы документооборота» [1]. А.Б. Смушкин исходит из необходимости сформировать экосистему предварительного расследования, отмечая, что «Электронное уголовное дело, которое должно формироваться в рамках рассматриваемой экосистемы, должно служить оптимизации уголовного судопроизводства и повышению эффективности расследования» [4].

В данной статье мы хотим обратить внимание на предупреждение преступлений, связанных с материалами уголовного дела и совершаемых сотрудниками правоохранительных и судебных органов. Такие факты, хотя их и нельзя признать распространенными, имеют место. Кроме того, данные деяния обладают высокой степенью латентности, поскольку зачастую должностное лицо «остается наедине» с документами, подшитыми в материал КУСП, надзорное производство или даже уголовное дело.

В 2024 году за совершение преступлений, предусмотренных частями 2 и 3 статьи 303 УК РФ (фальсификация доказательств по уголовному делу лицом, производящим дознание, следователем, прокурором или защитником), было осуждено соответственно 27 и 24 лица [3]. В основном (соответственно 12 и 22 лица) эти лица относятся к категории «прокуроры, следователи». Возможна квалификация незаконных действий с материалами уголовного дела и по другим статьям УК РФ (285, 286, 292, 294 УК РФ),

например, когда документы, находящиеся в деле, не являются доказательствами и не содержат доказательства.

С данной точки зрения использование новых информационных систем для ведения уголовного судопроизводства можно рассматривать как техническую меру предупреждения преступности. Такие меры имеют зачастую очень высокую эффективность. Л.Р. Клебанов в этой связи отмечал, что «в настоящее время, когда преступный мир берет на вооружение все актуальные достижения человечества, техническое противодействие преступности является зачастую решающим. Необходимыми знаниями о технических мерах противодействия преступности, аппаратах, механизмах и технологиях, которые используются для предупреждения преступности, должны обладать все специалисты, вовлеченные в процесс борьбы с преступностью в целом и отдельными группами преступлений» [2]. Действительно, в ряде случаев гораздо проще сделать технически невозможным совершение какого-либо преступления или, по крайней мере, усложнить его совершение, чем долго и порою безуспешно привлекать совершивших данное деяние лиц к уголовной и иным видам ответственности.

Такой технической мерой является цифровизация производства по уголовному делу. При последовательной и эффективной реализации она позволит устранить причины и условия, способствующие совершению преступлений, связанных с материалами уголовного дела.

Цели фальсификации материалов уголовного дела или, до этого, материалов проверки сообщения о преступлении на стадии возбуждения уголовного дела, могут быть различные. При этом они не обязательно являются корыстными. Зачастую следователь, дознаватель, оперативный работник вносит искусственные изменения в материалы уголовного дела с целью улучшить положение дел, исправить статистику по отделу, произвести впечатление на руководство, создать имидж компетентного сотрудника и тому подобное. Большое значение при этом имеет уровень раскрываемости преступлений. Регистрация сообщения о преступлении в книге учета сообщений о происшествиях не всегда может окончится раскрытием преступления, его расследованием и вынесением обвинительного приговора. Зачастую проверка сообщения о преступлении оканчивается постановлением об отказе в возбуждении уголовного дела.

Другой встречающейся ситуацией являются случаи возбуждения уголовного дела в отношении конкретного лица. При этом в последующем выясняется, что данное лицо непричастно к совершению этого преступления. На практике имеют место случаи замены постановления о возбуждении уголовного дела на вновь созданное постановление, в котором дело возбуждено не в отношении конкретного лица, а по какому-либо факту. Это исключает, в частности, обращение лица с заявлением о реабилитации и, как следствие, выплату ему определенной суммы. Для следователя это означает возможное дисциплинарное взыскание.

С целью избежания такой ситуации некоторые недобросовестные должностные лица могут пойти на замену материалов уголовного дела. При этом помимо постановления о возбуждении уголовного дела заменены могут быть и другие документы.

Представляется, что в данном случае само совершение преступления существенно усложнилось бы, если бы использовалось электронное уголовное дело. Кроме того, само осознание следователем того факта, что имевшую место фальсификацию можно было бы выявить с помощью двух-трех кликов на компьютере судьи, надзирающего прокурора, руководителя следственного органа или представителя потерпевшего, остановило бы следователя от попыток подобным образом уменьшить объем работы, упростить, ускорить работу или приукрасить действительное положение дел по службе.

При этом, естественно, необходимо параллельно принимать активные меры по борьбе с «палочной системой», «борьбой за раскрываемость», сравнением с аналогичным периодом прошлого года и т.п. Эффективность работы органов предварительного расследования не должна измеряться с помощью таких грубых показателей. Должна быть комплексная разносторонняя оценка эффективности следственных подразделений на основе разных показателей и раскрываемость, количество направленных в суд дел не должны быть здесь на первом месте.

Заключение. Внедрение электронного уголовного дела и его материальной основы, единой платформы электронного уголовного судопроизводства, среди многих других преимуществ имеет большое профилактическое значение в деле борьбы с преступлениями сотрудников правоохранительных и судебных органов. Отображение всех процессуальных действий по уголовному делу, принятия всех процессуальных решений и иных документов усложнит или сделает вообще невозможным рассматриваемые деяния.

Список литературы

1. Гаврилов М.А. Перспективы использования информационных технолоий в уголовном судопроизводстве в контексте реализации прокурорских полномочий // Российский следователь. 2024. № 11. С. 10–14.

2. Клебанов Л.Р. Технические меры предупреждения преступности: понятие, виды и субъекты применения // Союз криминалистов и криминологов. 2021. № 2. С. 7–20.

3. Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. Электронный ресурс: https://cdep.ru/ (дата обращения: 03.07.2025).

4. Смушкин А.Б. Экосистема предварительного расследования // Актуальные проблемы российского права. 2023. № 7. С. 143–158.

УДК 343

В. Ф. Васюков,
доктор юридических наук, профессор,
Московская академия Следственного комитета Российской Федерации
имени А. Я. Сухарева,
В. Н. Чаплыгина,
кандидат юридических наук, доцент,
Орловский юридический институт МВД России
имени В. В. Лукьянова

Сравнительный анализ методов легализации преступных доходов: система «хавала» и криптовалютное смешивание

Аннотация. В настоящей статье проводится сравнительный анализ двух разнородных, но функционально эквивалентных механизмов легализации (отмывания) преступных доходов: традиционной неформальной системы денежных переводов «Хавала» и современного технологического инструментария, известного под термином «криптовалютное смешивание». Целью исследования является выявление сущностных характеристик, общих черт и принципиальных различий данных феноменов. На основании проведенного анализа формулируются выводы о необходимости разработки междисциплинарных мер противодействия, адекватных вызовам гибридных финансовых схем.

Ключевые слова: легализация доходов, отмывание денег, Хавала, миксинг, финансовые преступления, псевдоанонимность

V. F. Vasyukov,
Doctor of Law, Professor,
Moscow Academy of the Investigative Committee
of the Russian Federation named after A. Ya. Sukharev,
V. N. Chaplygina,
Candidate of Law, Associate Professor,
Oryol Law Institute of the Ministry
of Internal Affairs of Russia named after V.V. Lukyanov

Comparative analysis of methods of legalization of criminal proceeds: the hawala system and cryptocurrency mixing

Abstract. This article provides a comparative analysis of two disparate but functionally equivalent mechanisms for legalization (laundering) of criminal proceeds: the traditional informal money transfer system "Hawala" and modern technological tools known under the term "cryptocurrency mixing". The purpose of the study is to identify the essential characteristics, common features and fundamental differences of these phenomena. Based on

the analysis, conclusions are drawn about the need to develop interdisciplinary countermeasures adequate to the challenges of hybrid financial schemes.

Keywords: legalization of income, money laundering, Hawala, mixing, financial crimes, pseudo-anonymity

Введение. Эволюция преступной деятельности в сфере финансовых операций демонстрирует высокую степень адаптивности к изменениям в нормативно-правовом регулировании и технологическом прогрессе. В контексте усиления международного контроля за финансовыми потоками наблюдается трансформация методов легализации преступных доходов, выражающаяся в переходе от традиционных схем к использованию цифровых технологий.

В связи с этим научный интерес представляет сопоставление устойчивой системы «Хавала» и относительно нового механизма криптовалютного смешивания. Исследование исходит из гипотезы о том, что указанные методы, несмотря на фундаментальные различия в технологической и организационной основе, выполняют идентичные функции в процессе отмывания денег и все чаще используются как гибридные модели незаконного оборота капитала.

Основная часть. *Система «Хавала»* (далее – хавала) представляет собой исторически сложившийся социальный институт, функционирующий на основе неформальных договоренностей и репутационных обязательств.

В то время как на Западе происходило становление формальных банковских систем, исторические корни хавалы предшествуют им на несколько столетий, беря начало в раннесредневековой торговле Ближнего и Среднего Востока. Ее возникновение связано с потребностью арабских торговцев безопасно перемещать свои богатства без физических тягот и риска ограбления на Шелковом пути. В арабском языке «Хавала» переводится как «платеж» или «перевод долга», что аналогично римскому понятию «делегация долга». Примечательно, что, войдя в хиндиязычный лексикон, оно приобрело дополнительную коннотацию «доверия» – неоценимого атрибута, остающегося фундаментом системы хавалы [9. С. 132].

В новейшее время мы наблюдаем трансформацию Хавалы под влиянием различных социально-политических и экономических факторов. В 1970-е годы, отмеченные нефтяным бумом на Ближнем Востоке, произошел рост исламских банков. Кроме того, операции по контрабанде золота между Ближним Востоком и Южной Азией в 1960-х годах привели к тому, что работавшие на Ближнем Востоке экспатрианты из Индии и Пакистана стали полагаться на хавалу для перевода средств своим семьям [7. С. 107].

В настоящее время хавала остается ключевым инструментом в рамках исламского коммерческого права, выступая как механизм передачи прав требований и осуществления платежей через посредников. Ее повсеместное распространение

на международном уровне даже привело к получению ею квази-легитимного статуса в таких регионах, как Южная Азия и Ближний Восток.

Таким образом, зародившись в средневековой торговле на Ближнем и Среднем Востоке, а также во времена династии Тан в Китае, хавала сегодня обрабатывает транзакции на сумму от 100 до 300 миллиардов долларов в год, работая параллельно с официальными финансовыми системами. Несмотря на то, что данная система играет жизненно важную роль для сообществ, не имеющих доступа к банковским услугам, особенно в Южной Азии и среди мигрантов по всему миру, она часто ассоциируется с преступной деятельностью, осуществляемой траснациональными организованными сообществами [8. С. 29].

Ее привлекательность для целей легализации доходов обусловлена следующими ключевыми характеристиками:

1) отсутствие физического перемещения средств. Операции осуществляются через систему взаимозачетов между агентами, что исключает необходимость трансграничной передачи наличности и минимизирует риски перехвата.

2) минимальная идентификация клиентов. Процедуры Know Your Customer (KYC) и Customer Due Diligence (CDD) отсутствуют, что обеспечивает высокий уровень конфиденциальности и затрудняет установление личности бенефициарных владельцев.

3) отсутствие формального документального следа. Операции фиксируются в устной форме или в несистематизированных учетных книгах, что создает непреодолимые препятствия для проведения финансового аудита и уголовно-процессуального расследования.

4) интеграция с легальным сектором экономики. Взаиморасчеты между хаваладарами часто маскируются под внешне законные коммерческие операции, такие как торговля товарами с заниженной или завышенной таможенной стоимостью, что обеспечивает видимость экономической обоснованности транзакций.

В рамках классической модели отмывания денег система «Хавала» наиболее эффективна на этапе интеграции, когда наличные средства, полученные преступным путем, вводятся в легальный финансовый оборот через приобретение активов или инвестирование в бизнес.

Между тем, *криптовалютное смешивание* представляет собой технологически сложный механизм, использующий возможности блокчейн-инфраструктуры для сокрытия следов незаконной деятельности. В своей основе этот процесс направлен на системное разрушение прозрачности и прослеживаемости транзакций, которые изначально заложены в публичных распределенных реестрах. Техническая реализация обфускации следов транзакций осуществляется через несколько взаимодополняющих методов [6].

Классическим и наиболее распространенным инструментом являются централизованные сервисы-миксеры, на которые поступают токены от разных пользователей, после чего они перемешиваются и выводятся на новые адреса

получателей в случайных, не связанных с входящими транзакциями суммах, что эффективно разрывает очевидную связь между точкой отправления и точкой назначения актива.

Более сложными и устойчивыми к контролю считаются децентрализованные миксеры, реализованные в виде смарт-контрактов на блокчейнах, так как их работа алгоритмизирована и не требует доверия к оператору, что исключает риски изъятия средств или компрометации со стороны самого сервиса.

Криптовалютное смешивание является одним из главных методов так называемого, «криптоотмывания» под которым понимается легализация незаконно полученных доходов посредством использования инфраструктуры криптоактивов [2. С. 18-24].

Данное явление характеризуется двумя основными сценариями происхождения преступных средств, которые условно обозначаются как «офф-чейн» и «он-чейн» активности.

Под «офф-чейн» активностью понимается генерация преступного дохода в рамках традиционной экономики, например, в результате незаконного оборота наркотических средств, торговли оружием или контрабанды. В данном случае криптовалюты выступают не как средство совершения преступления, а как инструмент последующей легализации: фиатные средства конвертируются в криптоактивы с целью обфускации их происхождения и последующей интеграции в легальный финансовый оборот.

Между тем, «он-чейн» активность предполагает, что преступный доход изначально возникает в цифровой среде и уже выражен в криптовалюте. Такие доходы, как правило, являются результатом киберпреступлений, в частности, атак с использованием программ-вымогателей, мошенничества в сфере первичных предложений монет (ICO), фишинга, а также продажи незаконных товаров и услуг на темных онлайн-рынках [4. С. 342].

В этом случае средства не требуют конвертации и сразу подвергаются процедурам обфускации через миксеры.

Рост популярности криптоактивов в качестве расчетного инструмента в криминальной среде обусловлен их псевдоанонимностью, глобальной доступностью, отсутствием централизованного контроля и высокой скоростью транзакций.

Вместе с тем, с теоретико-правовой точки зрения, криптоотмывание не следует рассматривать как принципиально новое преступное явление. Как справедливо отмечает вьетнамский исследователь Сюань Ту Тран, «данное явление представляет собой адаптацию традиционных методов отмывания денег к новым технологическим реалиям» [10].

Его основные характеристики включают:

1) использование инструментов обфускации. Применение криптомиксеров, децентрализованных бирж и кросс-чейн бриджей позволяет разорвать связь между исходным и конечным адресами кошельков, затрудняя трассировку транзакций.

2) псевдоанонимность. Несмотря на публичную природу блокчейна, привязка криптографических адресов к реальным личностям является сложной задачей, требующей применения специализированных методов анализа транзакционных графов.

3) высокая скорость и глобальная доступность. Операции совершаются в режиме реального времени и не зависят от географических границ или часовых поясов.

Ключевая уязвимость криптовалютного процессинга как метода легализации доходов заключается в его зависимости от точек входа и выхода (on/off-ramps). Несмотря на высокую степень анонимности и децентрализации внутри самой блокчейн-системы, процесс конвертации традиционных фиатных денег в криптовалюту и, что особенно важно, обратная конвертация отмытых активов в легальные фиатные средства требуют взаимодействия с централизованными платформами [5. С. 267].

Что касается функционального применения в процессе отмывания, криптовалютный процессинг демонстрирует наибольшую эффективность на начальных и промежуточных стадиях. На этапе размещения он позволяет анонимно внести изначально «грязные» фиатные средства, полученные преступным путем, в цифровую экосистему через уязвимые или нерегулируемые «on-ramp» сервисы [3. С. 90].

На последующем этапе подмены его инструментарий становится центральным: средства подвергаются сложной многоэтапной обфускации. Этот процесс, как раз таки, включает многократные переводы между кошельками, использование миксеров для разрыва связей между адресами, конвертацию между различными криптоактивами и использование децентрализованных протоколов, что в совокупности направлено на создание непреодолимых сложностей для трассировки первоначального источника средств. Однако финальная стадия интеграции - преобразование «очищенных» криптоактивов в легальный фиат - вновь возвращает процесс к его ключевой уязвимости: необходимости пройти через регулируемые off-ramp точки выхода

Тот факт, что операции с криптовалютами происходят в киберпространстве, определяет необходимость изменения оперативной и следственной тактики, значительно усовершенствовать методы и инструменты раскрытия и расследования криптопреступлений. В том числе это обосновывается тем, что как таковое, место совершения преступления, в данном случае определяется множеством критериев и факторов (расположение сервера, адрес криптобиржи, тип кошелька и т.д.). В отдельных случаях определить конкретное место преступления не представляется возможным в силу технологических особенностей.

В связи с этим, как нами уже упоминалось в одной из работ, эффективность раскрытия и расследования преступлений, связанных с криптовалютами, во многом зависит от того, насколько уполномоченные субъекты смогли адаптироваться к новой технологической реальности, в которой им приходится работать [1. С. 74-76].

Анализ современной практики свидетельствует о формировании тенденции к синтезу традиционных и цифровых методов легализации доходов. Данная конвергенция проявляется в следующих формах:

1. Использование криптовалют в системе «Хавала». Хаваладары все чаще используют стейблкоины (USDT, USDC) для проведения взаиморасчетов между агентами. Это позволяет ускорить операции, снизить риски, связанные с физической транспортировкой наличных, и замаскировать транзакции под легальную криптовалютную активность.

2. Использование неформальных каналов для финальной интеграции криптоактивов. После обфускации в блокчейне «очищенные» криптовалютные активы конвертируются в фиатные деньги через нерегулируемые peer-to-peer (P2P) платформы или обналичиваются через сети, аналогичные «Хавале», в юрисдикциях с минимальным уровнем AML-контроля.

3. Использование NFT как инструмента гибридной схемы. Преступные структуры приобретают NFT за «грязные» криптовалюты через миксеры, после чего «продают» их себе же через фиктивные аккаунты за «чистые» средства, которые впоследствии выводятся через неформальные каналы.

Таким образом, формируется новая, гибридная модель, в которой технологии и традиции взаимно усиливают друг друга, создавая высокоустойчивые схемы, способные эффективно обходить как традиционные, так и цифровые механизмы контроля.

Заключение. Проведенный анализ позволяет сделать вывод о том, что системы «Хавала» и криптовалютное смешивание, несмотря на радикальные различия в своей технологической и организационной основе, являются функциональными аналогами в процессе легализации преступных доходов. Обе системы направлены на достижение максимальной непрозрачности финансовых операций, используя различные механизмы: первая – за счет минимизации документальной фиксации и опоры на социальные связи, вторая – за счет технологической сложности отслеживания и псевдоанонимности.

Список литературы

1. Васюков В. Ф., Старжинская А.Н. Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют // Российское право: образование, практика, наука. 2024. № 4. С. 68-78.

2. Волеводз А.Г. Международно-правовое регулирование возврата преступных активов в рамках БРИКС: современное состояние и перспективы // Актуальные

проблемы международного сотрудничества в борьбе с преступностью : Сборник научных трудов Международной научно-практической конференции, Москва, 16 ноября 2023 года. Москва: Московский университет МВД РФ им. В.Я. Кикотя, 2023. С. 18-24.

3. Колычева, А. Н., Васюков В. Ф. Отдельные аспекты противодействия использованию криптовалют в преступных целях // Криминалистика: вчера, сегодня, завтра. 2025. № 1(33). С. 89-101.

4. Преступления в сфере высоких технологий и информационной безопасности / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина. – Москва : Общество с ограниченной ответственностью "Издательство Прометей", 2023. 1086 с.

5. Противодействие криптовалютным преступлениям в зарубежных странах / В. Ф. Васюков, А. Г. Волеводз, К. К. Клевцов [и др.]. – Москва : ООО Издательский дом "Юрлитинформ", 2025. 504 с.

6. Illicit Financial Flows from Cyber-Enabled Fraud / FATF – Interpol - Egmont Group // FATF. – Paris, France. – 2023. – URL: www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyberenabled-fraud.html

7. Kanellopoulos A. N. The Hawala System in the Western Balkans: Challenges and Strategies for Counterterrorism and Counterintelligence //Romanian Intelligence Studies Review. 2024. №. 1 (31). С. 103-124.

8. Moin B. Taming the untamable: Rethinking, regulating, and revamping hawala //Journal of Academics Stand Against Poverty. 2024. Т. 5. №. 1.С. 20-43.

9. Rahimi H. How to create better Hawala regulations: a case study of Hawala regulations in Afghanistan //Crime, Law and Social Change. 2021. Т. 76. – №. 2. С. 131-148.

10. Tran Tu X. Money Laundering Risks in Decentralized Finance: Reassessing the EU Anti-Money Laundering Framework forCrypto-Assets in light of Legal Certainty and Effective Enforcement. 2025.

УДК 343.3/.7

А. В. Волкова,
соискатель кафедры уголовного права и процесса
Казанского инновационного университета
имени В.Г. Тимирясова

Исключение из сферы действия статьи 272[1] УК РФ: обработка персональных данных для личных и семейных нужд

Аннотация. Критическому анализу подвергается примечание 1 к статье 272[1] Уголовного кодекса Российской Федерации, устанавливающее исключение из сферы действия уголовно-правовой нормы обработки персональных данных физическими лицами исключительно для личных и семейных нужд, что требует разграничения личной и профессиональной деятельности в цифровой среде. Указание в примечании на физических лиц ориентирует на то, что оно не распространяется на лиц, которым такие сведения были доверены (доступны) в рамках осуществления служебной или иной профессиональной деятельности.

Ключевые слова: субъект преступления, ст. 272[1] УК РФ, общий субъект, специальный субъект, персональные данные, возраст уголовной ответственности, физическое лицо, цифровая идентичность, анонимность

A. V. Volkova,
Candidate of the Department of Criminal Law and Procedure
Kazan Innovative University
named after V.G. Timiryasov

Exclusion from the scope of article 272[1] of the Criminal Code of the Russian Federation: processing of personal data for personal and family needs

Annotation. Note 1 to Article 272[1] of the Criminal Code of the Russian Federation is being critically analyzed, which establishes an exception to the scope of the criminal law norm for processing personal data by individuals exclusively for personal and family needs, which requires a distinction between personal and professional activities in the digital environment. The reference in the note to individuals indicates that it does not apply to persons to whom such information was entrusted (available) in the framework of their official or other professional activities.

Keywords: subject of crime, Article 272[1] of the Criminal Code of the Russian Federation, general subject, special subject, personal data, age of criminal responsibility, individual, digital identity, anonymity

Введение. Федеральным законом от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» [1] установлена ответственность

за незаконный оборот персональных данных (ст. 272[1] УК РФ). Указанные изменения ознаменовали новый этап развития уголовно-правовой охраны персональных данных в российской правовой системе, что актуализирует необходимость фундаментального переосмысления категорий объекта и предмета данного состава преступления в контексте существенного расширения диапазона криминализированных деяний и усложнения их квалифицирующих признаков [3. С. 86-95].

Основная часть. Хотелось бы остановиться на одной из особенностей конструирования уголовно-правового запрета, которое вызывает множество дискуссий. Так, примечанием 1 к ст. 272[1] УК РФ устанавливает специфическое исключение: «Действие настоящей статьи не распространяется на случаи обработки персональных данных физическими лицами исключительно для личных и семейных нужд». По мнению Е.А. Русскевича, законодатель формулирует не обстоятельство, исключающее преступность деяния, а универсальный критерий малозначительности. Смысл данного примечания заключается в том, чтобы исключить из сферы уголовной репрессии «бытовое» распространения персональных данных друзей, коллег и знакомых, когда лицо не утруждает себя тем, чтобы истребовать на это необходимое согласие субъекта персональных данных [4. С. 53-59]. Данная норма создает ситуацию, когда определенная категория физических лиц при наличии всех объективных и субъективных признаков состава преступления освобождается от уголовной ответственности в силу особого характера деятельности по обработке персональных данных. Скорее всего законодатель посчитал то, что такое деяние не обладает именно той общественной опасностью, свойственной преступлению.

Примечание 1 к ст. 272[1] УК РФ воспроизводит положение ч. 1 ст. 1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [2] (далее – Федеральный закон № 152-ФЗ «О персональных данных»), согласно которому действие данного закона не распространяется на отношения, возникающие при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных. Исключение обработки персональных данных для личных и семейных нужд из сферы регулирования законодательства о персональных данных обусловлено признанием того, что частная жизнь граждан, их личные и семейные отношения относятся к автономной сфере, в которую государство не должно чрезмерно вмешиваться, устанавливая детальные требования к обработке информации.

Важным является определение содержания понятий «личные нужды», «семейные нужды» и критерия «исключительности» обработки персональных данных для таких нужд. Федеральный закон № 152-ФЗ «О персональных данных» не содержит легального определения данных понятий, что требует доктринального толкования с учетом целей правового регулирования.

Личные нужды означают потребности физического лица, связанные с его частной жизнью, не связанные с профессиональной, коммерческой, публичной

деятельностью: ведение личных записей, дневников, личной переписки; хранение контактов знакомых, коллег, партнеров в адресных книгах, на мобильных устройствах; создание личных фотоальбомов, видеоархивов; ведение личных финансовых записей, учета расходов; использование персональных данных для организации личного досуга, путешествий, хобби.

Семейные нужды охватывают обработку персональных данных членов семьи для целей, связанных с семейной жизнью: хранение семейных фотографий, видеозаписей; ведение семейных архивов, генеалогических записей; организация семейных мероприятий, праздников; ведение семейного бюджета, финансового планирования; координация семейной деятельности, коммуникации между членами семьи.

Критерий «исключительности» означает, что обработка персональных данных должна осуществляться только для личных и семейных нужд, без какой-либо профессиональной, коммерческой, публичной составляющей. Если обработка персональных данных хотя бы частично связана с профессиональной деятельностью, предпринимательством, публичной активностью, исключение не применяется.

Типичные ситуации, когда обработка персональных данных не может считаться исключительно для личных и семейных нужд: ведение базы данных клиентов для предпринимательской деятельности, даже осуществляемой в малом масштабе, без регистрации юридического лица или индивидуального предпринимателя; публикация персональных данных третьих лиц в социальных сетях, блогах, на публичных интернет-ресурсах; сбор персональных данных для последующей передачи работодателю, государственным органам, коммерческим организациям; обработка персональных данных в рамках профессиональной деятельности (например, фотограф, обрабатывающий персональные данные клиентов).

Применительно к ст. 272^1 УК РФ примечание 1 создает специфическую ситуацию: физическое лицо может совершить действия, формально содержащее все признаки состава преступления (использование, передачу, сбор, хранение компьютерной информации, содержащей персональные данные, полученной незаконным путем), но если эти действия осуществляются исключительно для личных и семейных нужд, то уголовная ответственность не наступает. Примером может служить ситуация, когда лицо получает доступ к личной переписке супруга, фотографиям на его компьютере или мобильном устройстве путем неправомерного доступа (подбор пароля, использование шпионского программного обеспечения) и сохраняет эту информацию для личного ознакомления в связи с подозрениями в супружеской неверности. Формально данные действия образуют состав преступления по ч. 1 ст. 272^1 УК РФ: имеет место хранение компьютерной информации, содержащей персональные данные (переписка, фотографии супруга), полученной путем неправомерного доступа (взлом устройства супруга). Однако примечание 1 к ст. 272^1 УК РФ исключает уголовную ответственность, поскольку обработка осуществляется для личных и семейных нужд.

Вместе с тем применение примечания 1 к ст. 272^1 УК РФ требует соблюдения критерия исключительности и учета оговорки Федерального закона № 152-ФЗ «О персональных данных» о недопустимости нарушения прав субъектов персональных данных. Если физическое лицо, получив персональные данные для личных или семейных нужд, затем использует их для иных целей (публикация в сети Интернет, передача третьим лицам, использование для причинения вреда), исключение не применяется, наступает уголовная ответственность по ст. 272^1 УК РФ. Например, лицо, получив путем неправомерного доступа интимные фотографии бывшего партнера, первоначально хранило их для личного просмотра, что подпадало под исключение примечания 1; однако затем разместило эти фотографии в социальных сетях, что образует состав преступления по ч. 1 ст. 272^1 УК РФ (передача – распространение персональных данных, полученных путем неправомерного доступа), исключение не применяется, поскольку обработка перестала быть исключительно для личных нужд.

Заключение

Примечание 1 к ст. 272^1 УК РФ исключает из сферы действия нормы обработку персональных данных физическими лицами исключительно для личных и семейных нужд, что отражает признание автономии частной жизни. Законодателем предполагается, что такие деяния не носят систематический и возмездный характер, а исходит из «бытовых» не этичных действий лица.

Вместе с тем применение данного исключения требует соблюдения критерия исключительности и недопустимости нарушения прав субъектов персональных данных.

Указание в примечании на физических лиц ориентирует на то, что оно не распространяется на лиц, которым такие сведения были доверены (доступны) в рамках осуществления служебной или иной профессиональной деятельности.

Список литературы

1. Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Собрание законодательства Российской Федерации. 2024. № 49 (ч. IV). Ст. 7412.

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3451.

3. Волкова А. В. Социальная обусловленность криминализации незаконных действий с компьютерной информацией, содержащей персональные данные // Проблемы права. 2025. № 4 (100). С. 86–95.

4. Русскевич Е. А. Об уголовной ответственности за незаконные действия с компьютерной информацией, содержащей персональные данные // Уголовный процесс. – 2025. – № 7(247). – С. 53-59. – EDN PYYGBX.

УДК 343.3/.7

А. В. Волкова,
соискатель кафедры уголовного права и процесса
Казанского инновационного университета
имени В.Г. Тимирясова

Проблемы разграничения состава преступления, предусмотренного статьей 272[1] УК РФ, со смежными составами преступлений

Аннотация: в представленной публикации формулируются практические рекомендации по квалификации преступлений, предусмотренных статьей 272[1] УК РФ, с учетом специфики объекта и предмета, предложения по разрешению конкуренции со смежными составами преступлений, определению границ уголовной ответственности. Квалификация деяний по ст. 272[1] УК РФ требует разграничения со смежными составами преступлений, имеющими сходные признаки объекта, предмета или объективной стороны. Законодательная конструкция состава преступления и отсутствие разъяснений Пленума Верховного Суда Российской Федерации создают проблемы в правоприменении.

Ключевые слова: объект преступления, предмет преступления, ст. 272[1] УК РФ, персональные данные, компьютерная информация, неприкосновенность частной жизни, информационная безопасность, биометрические данные, специальные категории персональных данных

A.V. Volkova,
Candidate of the Department of Criminal Law and Procedure
Kazan Innovative University
named after V.G. Timiryasov

Problems of distinguishing the corpus delicti provided for in article 2721 of the criminal code of the russian federation with related corpus delicti

Abstract: practical recommendations are formulated on the qualification of acts, taking into account the specifics of the object and subject, the resolution of competition with related crimes, and the definition of the boundaries of criminal responsibility. The qualification of acts under Article 272[1] of the Criminal Code of the Russian Federation requires differentiation from related crimes that have similar features of the object, subject or objective side. The legislative structure of the corpus delicti and the lack of explanations from the Plenum of the Supreme Court of the Russian Federation create problems in law enforcement.

Keywords: object of crime, subject of crime, Article 272[1] of the Criminal Code of the Russian Federation, personal data, computer information, privacy, information security, biometric data, special categories of personal data

Введение. Квалификация деяний по ст. 272[1] УК РФ требует разграничения со смежными составами преступлений, имеющими сходные признаки объекта, предмета или объективной стороны.

Наиболее актуальным является разграничение ст. 272[1] УК РФ со ст. 137 УК РФ о нарушении неприкосновенности частной жизни, ст. 272 УК РФ о неправомерном доступе к компьютерной информации, ст. 183 УК РФ о незаконных получении и разглашении сведений, составляющих коммерческую, налоговую или банковскую тайну.

Основная часть.

Рассмотрим соотношение состава преступления, предусмотренного ст. 272[1], со ст. 137 УК РФ, которая уже поднималась авторами [3. С. 125-126]. Считаем, что их стоит рассматривать как общую и специальную норму и при возникновении конкуренции применять специальную норму. Так, ст. 137 УК РФ устанавливает ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Объектом ст. 137 УК РФ является конституционное право на неприкосновенность частной жизни, личную и семейную тайну. Предметом являются сведения о частной жизни лица, составляющие его личную или семейную тайну, независимо от формы их представления: устная информация, печатные документы, рукописи, фотографии на бумажных носителях, аналоговые аудио- и видеозаписи, компьютерная информация. Ст. 272[1] УК РФ является специальной нормой по отношению к ст. 137 УК РФ применительно к конкретизации предмета преступления – компьютерная информация, содержащая персональные данные. Критерием разграничения является форма представления информации: если деяние совершается с компьютерной информацией, содержащей персональные данные, применяется ст. 272[1] УК РФ как специальная норма; если с информацией о частной жизни в иной форме – применяется ст. 137 УК РФ.

Мы поддерживаем мнение Е.А. Русскевича о том, что с учетом единства умысла квалифицировать содеянное, когда лицо часть сведений предоставило посредством отправки фотографий монитора компьютера (скриншотов), а часть по причине значительного объема данных передало на бумаге, необходимо только по норме, которая предусматривает более тяжкий состав преступления, то есть по ст. 272[1] УК РФ [2].

Соотношение ст. 272[1] и ст. 272 УК РФ о неправомерном доступе к компьютерной информации определяется различием в объективной стороне и предмете [1. С. 22]. Кроме того, законодателем сделана оговорка в ст. 272 УК РФ, что применяется ст. 272[1] УК РФ, если предметом преступления являются персональные данные. Предметом преступления в ст. 272 УК РФ является охраняемая законом компьютерная информация (независимо от содержания). В свою очередь ст. 272[1]

УК РФ криминализирует не сам доступ к информации, а последующие действия с информацией, полученной незаконным путем: использование, передачу, сбор, хранение. Предметом преступления в ст. 272^1 УК РФ является специфический вид компьютерной информации – информация, содержащая персональные данные.

Ст. 272 УК РФ криминализирует неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (материальный состав, требующий наступления общественно опасных последствий). Объективная сторона состава преступления, предусмотренного ст. 272 УК РФ, заключается в неправомерном доступе – получении возможности ознакомления с информацией и (или) ее использования путем преодоления системы защиты. Ст. 272^1 УК РФ не требует наступления последствий, которые отмечены в ст. 272 УК РФ.

Соотношение норм может быть следующим: неправомерный доступ к компьютерной информации, содержащей персональные данные, с последующим использованием или передачей этой информации образует совокупность преступлений, предусмотренных ст. 272 и 272^1 УК РФ.

При этом неправомерный доступ к компьютерной информации, не содержащей персональных данных, квалифицируется только по ст. 272 УК РФ; использование или передача компьютерной информации, содержащей персональные данные, полученной законным путем, но используемой незаконно, квалифицируется только по ст. 272^1 УК РФ.

Заключение.

Квалификация деяний по ст. 272^1 УК РФ требует разграничения со смежными составами преступлений, имеющими сходные признаки объекта, предмета или объективной стороны. Законодательная конструкция состава преступления и отсутствие разъяснений Пленума Верховного Суда Российской Федерации создают проблемы в правоприменении.

Список литературы

1. Бегишев И. Р. Уголовно-правовая характеристика преступлений против безопасности персональных данных: анализ статьи 2721 уголовного кодекса Российской Федерации / И. Р. Бегишев, Н. Н. Рыбушкин // Вестник Дальневосточного юридического института МВД России имени И.Ф. Шилова. – 2025. – № 4(73). – С. 19-23. – EDN SGDXFX.

2. Русскевич Е. А. Об уголовной ответственности за незаконные действия с компьютерной информацией, содержащей персональные данные // Уголовный процесс. – 2025. – № 7(247). – С. 53-59. – EDN PYYGBX.

3. Шутова А. А. Новеллы уголовного законодательства об ответственности за незаконный оборот персональных данных // Ученые записки Казанского университета. Серия: Гуманитарные науки. – 2024. – Т. 166, № 6. – С. 122-134. – DOI 10.26907/2541-7738.2024.6.122-134. – EDN LXPPWK.

УДК 343.3/.7

А. Н. Вострова,
аспирант,
Московский государственный юридический университет
имени О.Е. Кутафина (МГЮА)

Уголовная ответственность за действия с вредоносными программами в странах БРИКС

Аннотация. Исследование посвящено сравнительно-правовому анализу уголовной ответственности за действия с вредоносными программами в странах БРИКС (Россия, Бразилия, Китай, Индия, ЮАР, Египет, Эфиопия, Иран, ОАЭ, Индонезия, Саудовская Аравия). В статье выявлены существенные особенности национальных законодательств, проанализированы подходы к квалификации вредоносных программ как самостоятельного предмета преступления и как орудия совершения иных киберпреступлений. Особое внимание уделено дуалистической природе правового регулирования.

Ключевые слова: компьютерные преступления; киберпреступление; вредоносная компьютерная программа; вредоносная компьютерная информация; информационная безопасность

A.N. Vostrova
Postgraduate student,
Kutafin Moscow state Law University (MSAL)

Criminal liability for actions with malware in BRICA countries

Absract. The study is devoted to the comparative legal analysis of criminal liability for actions with malicious programs in the BRICS countries (Russia, Brazil, China, India, South Africa, Egypt, Ethiopia, Iran, UAE, Indonesia, Saudi Arabia). The article identifies significant features of national legislation, analyzes approaches to the qualification of malicious programs as an independent subject of a crime and as a tool for committing other cybercrimes. Particular attention is paid to the dualistic nature of legal regulation.

Keywords: computer crimes; cybercrime; malicious computer program; malicious computer information; information security

Введение

В контексте стремительной цифровизации экономик и роста зависимости обществ от информационно-коммуникационных технологий (далее – ИКТ) вопросы обеспечения безопасности в цифровой среде выходят на первый план. В Декларации Рио-де-Жанейро [1. С.13,16], принятой по итогам XVII саммита БРИКС, подчеркивается, что государства-участники объединения демонстрируют твердую

приверженность укреплению многостороннего сотрудничества в сфере безопасности и противодействия транснациональным вызовам, среди которых киберпреступность занимает одно из ключевых мест.

Участники БРИКС выражают уверенность в необходимости создания открытой, безопасной, стабильной и доступной среды ИКТ, что напрямую связано с противодействием использованию вредоносных программ, представляющих серьезную угрозу как для безопасности государств, так и для прав граждан. В связи с этим небезынтересно рассмотреть, как именно уголовная ответственность за действия с вредносными компьютерными программами определена в национальном законодательстве стран-участниц объединения (Россия, Бразилия, Китай, Индия, ЮАР, Египет, Эфиопия, Иран, ОАЭ, Индонезия, Саудовская Аравия).

Основная часть

В России уголовная ответственность за создание, использование или распространение вредоносных компьютерных программ предусмотрена в ст. 273 УК РФ (за аналогичные действия с отдельными вредоносными компьютерными программами – в ч. 1 ст. 274^1 УК РФ). Однако нельзя не отметить тот факт, что вредоносные программы выступают не только предметом преступного посягательства, но и орудием (средством), с помощью которого можно совершить многие другие противоправные деяния [2. С. 168].

Уголовная ответственность за действия с вредоносными программами в Бразилии регламентируется уголовным законом, который выделяет данные преступления в отдельные составы. Необходимо обратить внимание, что в Уголовном кодексе Бразилии (далее – УК Бразилии) [10] не содержится самостоятельной главы, посвященной компьютерным преступлениям. Уголовная ответственность за данные деяния распределена по разным разделам УК Бразилии: ст. 154-А в разделе I «Преступления против личности», ст. 313-В в разделе XI «Преступления против государственной администрации».

Основной нормой является ст. 154-А, которая криминализирует вторжение в чье-либо компьютерное устройство, подключенное или не подключенное к сети, посредством неправомерного нарушения механизма безопасности. Целью такого вторжения является получение, изменение или уничтожение данных без разрешения владельца либо установка уязвимостей для получения неправомерной выгоды. Основной состав является функциональным аналогом ст. 272 УК РФ, так как предусматривает наказание за сам акт взлома и последующие действия с данными. В то же время § 1 этой же статьи прямо криминализирует создание и распространение «компьютерного устройства или программу с намерением…» для совершения таких действий, что непосредственно направлено против оборота вредоносных программ и является близким аналогом ст. 273 УК РФ. Таким образом, бразильский законодатель объединил в одной норме составы, которые в российской правовой системе представлены двумя отдельными составами.

Специальная норма, предусмотренная ст. 313-B, позволяет квалифицировать действия государственных служащих, которые без разрешения компетентного органа власти модифицируют информацию или оказывают иное негативное воздействие на информационные системы или программное обеспечение.

Можно сказать, что бразильское законодательство являет собой пример комплексного правового барьера против создания и использования вредоносного программного обеспечения, защищающего как частные права граждан на конфиденциальность и целостность данных, так и интересы государства и публичных служб.

В Китайской Народной Республике (далее – КНР) нормы предусматривающие уголовную ответственность за преступления в сфере ИКТ закреплены в Уголовном кодексе КНР (далее – УК КНР) [9]. Первоначальная регламентация действий с вредоносными программами была сосредоточена в ст. 286 УК КНР, но в последующем ст. 285 УК КНР была дополнена квалифицирующими признаками, в частности ч. 3 ст. 285 УК КНР, которая установила ответственность за создание и сбыт вредоносных программ или технических устройств, предназначенных для несанкционированного (вторжения) в компьютерные системы или для осуществления незаконного контроля над ними [5].

В Индии правовое регулирование уголовной ответственности за преступления в сфере ИКТ закрепляется в нескольких нормативно-правовых актах [3. С. 119-120]. Закон Индии № 21 от 09.06.2000 «Об информационных технологиях» (далее – Закон Индии) предусматривает уголовную ответственность за противоправные действия с компьютерными программами, которая содержится Главе XI, озаглавленной «Преступления» [15].

Статья 65 Закона Индии устанавливает запрет на определенные действия с исходным кодом. В соответствии с ее положениями, любое лицо, которое умышленно уничтожает или изменяет, либо умышленно заставляет другое лицо уничтожить или изменить «исходный код», используемый для компьютера, компьютерной программы, компьютерной системы или компьютерной сети, при условии что хранение или поддержание указанного «исходного кода» требуется в силу действующего законодательства, подлежит уголовному преследованию.

Важно отметить, что законодатель дает легальное определение ключевого термина: под «исходным кодом компьютера» понимается «перечень программ, компьютерных команд, дизайн и компоновка, а также программный анализ компьютерного ресурса в любой форме», что расширяет объективную сторону преступления и охватывает различные формы представления кода». Норма направлена на защиту целостности и сохранности критически важной цифровой информации, подлежащей обязательному хранению, и является частью правового механизма противодействия киберпреступности в Индии.

В Южно-Африканской Республике важнейшим инструментом противодействия киберпреступности является Закон № 19 от 2020 г. «О киберпреступлениях» [10], который закрепляет широкий спектр общественно опасных посягательств в сфере ИКТ [4, С. 1091]:

– статья 4 (1) криминализирует незаконное владение или использование любого программного обеспечения или устройства, созданного для нарушения других положений Закона, например, для доступа или перехвата данных;

– статья 5 (1) определяет вмешательство в данные или программу как их удаление, изменение, повреждение или блокировку доступа, делающее их бесполезными;

– статья 6 защищает компьютерные системы и носители от вмешательства, нарушающего их функционирование, целостность или доступность;

– статья 7 запрещает незаконные приобретение, хранение или использование паролей и кодов доступа.

В Египте уголовная ответственность за компьютерные преступления определена в Законе от 2018 года № 175 «О преступлениях против кибербезопасности и информационных технологий» (далее – Закон Египта) [13].

В соответствии со ст. 22 любые незаконные действия с аппаратным и программным обеспечением, специально разработанным или адаптированным для совершения компьютерных атак, являются преступлением. Под действие этой статьи подпадают изготовление, импорт, экспорт, продажа, приобретение, владение или распространение любых устройств, оборудования, инструментов, компьютерных программ, кодов доступа, шифров или аналогичных данных без разрешения уполномоченного органа (Национального управляющего органа по регулированию связи – NTRA), если доказано, что эти действия были совершены с целью их использования для совершения или облегчения совершения любого преступления, предусмотренного Законом, либо для сокрытия его следов. Таким образом, сам факт создания или распространения вредоносного программного обеспечения, независимо от его последующего использования, является уголовно наказуемым деянием.

Одновременно с этим вредоносные программы выступают в качестве основного орудия совершения множества других преступлений, описанных в Законе Египта. Например, ст. 17 предусматривает ответственность за умышленное и неправомерное уничтожение, повреждение, изменение, блокирование или удаление – полностью или частично – программ или данных, хранящихся, обрабатываемых или передаваемых в любой информационной системе. Совершение этих действий практически невозможно без использования специализированного вредоносного программного обеспечения, такого как шифровальщики, стейлоры или деструктивные вирусы.

Атаки на целостность и доступность информационных сетей, криминализированные ст. 21, также практически всегда осуществляются с применением вредоносных программ. К ним относятся DDoS-атаки с

использованием ботнетов, распространение сетевых червей и другие действия, направленные на вывод сети из строя, нарушение ее эффективности, создание помех или перехват обработки данных. Санкции за такие действия ужесточаются, если атаке подверглась сеть, принадлежащая государству или государственному юридическому лицу.

Кроме того, вредоносные программы являются инструментом для совершения преступлений, связанных с несанкционированным доступом (ст. 14), перехватом данных (ст. 16), посягательством на электронную почту и частные счета (ст. 18), а также мошенничеством с использованием платежных карт и электронных средств платежа (ст. 23). В последнем случае вредоносные программы, такие как банковские трояны и кейлоггеры, используются для незаконного получения реквизитов карт с целью последующего хищения денежных средств.

Закон Египта также ужесточает наказание, если преступление совершено с использованием вредоносных программ в определенных целях. Статья 34 определяет квалифицирующий состав: если любое из преступлений, предусмотренных Законом Египта, совершено с целью подрыва общественного порядка, угрозы безопасности общества, нанесения ущерба национальной безопасности, экономическому статусу страны, препятствования работе государственных органов или нанесения ущерба национальному единству.

Важно отметить, что Закон Египта устанавливает ответственность не только для физических, но и для юридических лиц (ст. 35, 36). Если преступление совершено от имени или в интересах компании, к уголовной ответственности может быть привлечено фактическое руководство, а суд вправе приостановить или аннулировать лицензию компании на осуществление деятельности.

Таким образом, египетский законодатель создал всеобъемлющую правовую базу для борьбы с киберпреступностью, где вредоносные программы рассматриваются двояко: как самостоятельный запрещенный предмет и как опасное орудие совершения других преступлений.

В 2016 году в Федеративной Республике Эфиопия был принят Закон от 07.07.2016 № 958/2016«О компьютерных преступлениях» (далее – Закон Эфиопии) [8] в котором закреплен ряд преступлений в сфере информационных технологий, в т.ч. за действия с вредоносными программами.

Так, в ст. 7 «Преступные деяния, связанные с использованием компьютерных устройств и данных» предусматривается уголовная ответственность за создание, распространение, передачу, приобретение или обладание вредоносными программами/устройствами/кодами, если они предназначены для повреждения/нарушения работы информационных систем.

Анализ эфиопского законодательства, в частности Закона Эфиопии, с точки зрения квалификации вредоносных программ как предмета и орудия преступления, позволяет выявить комплексный подход законодателя к криминализации данной

сферы. Вредоносные программы рассматриваются в законе в двух основных аспектах: как самостоятельный предмет противоправного посягательства и как инструмент для совершения других компьютерных и традиционных преступлений.

С одной стороны, вредоносные программы выступают предметом преступления, когда речь идет об их создании, распространении, использовании или хранении с противоправными целями. Статья 7 закона напрямую криминализирует умышленную передачу компьютерных программ, специально разработанных или адаптированных для причинения ущерба компьютерной системе, данным или сети, даже если такой ущерб в итоге не был причинен. Сам факт создания или распространения такой программы рассматривается как оконченное деяние, что подчеркивает его опасность как самостоятельного предмета преступного посягательства. Законодатель фокусируется на потенциальной вредоносности программы, а не только на фактических последствиях ее создания, распространия или даже использования.

С другой стороны, вредоносные программы являются ключевым орудием целого ряда квалифицированных преступлений, предусмотренных законом: несанкционированный доступ (ст. 3), вмешательство в работу компьютерной системы (ст. 5), причинение ущерба компьютерным данным (ст. 6) или компьютерный мошенничество (ст. 10). В этих случаях вредоносная программа не является конечной целью злоумышленника, а служит техническим средством для достижения иных преступных целей: получения доступа, нарушения работы, уничтожения данных или хищения имущества.

Эфиопский законодатель также вводит понятие «критической инфраструктуры», атака на которую с использованием вредоносных программ влечет более строгую уголовную ответственность. Это указывает на понимание того, что вредоносные программы как орудие может быть направлено против объектов, нарушение работы которых создает угрозу национальной и общественной безопасности.

В Иране уголовная ответственность за действия с вредоносными программами содержится в Законе от 26.05.2009 № 71063«О компьютерных преступлениях» (далее – Закон Ирана) [14]. В статье 25 главы 7 предусматривается ответственность за изготовление, предоставление, распространение или сбыт программ, устройств, паролей, средств, предназначенных для совершения преступлений, а также за иные «вспомогательные» деяния, связанные с компьютерными преступлениями.

В Объединенных Арабских Эмиратах (далее – ОАЭ) действует Федеральный декрет – Закон от 2021 г. № 34«О противодействии слухам и киберпреступности» [11]. В этом законе прямо предусмотрена уголовная ответственность за преступления в сфере ИКТ, в том числе за действия с вредоносными программами. Так, ст. 16 криминализирует сам факт ее написания или наличия на устройстве с преступным умыслом формирует оконченный состав преступления, даже если эта программа ни разу не была запущена против реальной цели.

Анализируя Закон Индонезии от 2008 года № 11 «Об электронной информации и транзакциях» (далее – Закон Индонезии) [12], с точки зрения уголовной ответственности за действия с вредоносными программами, можно выделить несколько ключевых аспектов, связанных с предметом и орудием совершения преступления.

Вредоносные программы рассматриваются в законе как инструмент (орудие) для совершения противоправных деяний, а также как самостоятельный предмет преступления, когда речь идет об их создании, распространении или использовании. Закон Индонезии не содержит отдельного определения вредоносных программ, но в рамках статей 27–37 описывает широкий спектр запрещенных действий, которые могут быть совершены с использованием таких программ.

С точки зрения орудия преступления вредоносные программы используются для доступа к компьютерным системам без разрешения (ст. 30), перехвата данных (ст. 31), изменения или уничтожения электронной информации (ст. 32), нарушения работы систем (ст. 33), а также для совершения мошеннических действий, клеветы, распространения запрещенного контента и других противоправных деяний. Например, ст. 35 прямо указывает на манипуляции с электронной информацией с целью придания ей видимости достоверности, что часто достигается именно с помощью вредоносных программ.

Как предмет преступления вредоносные программы подпадают под действие ст. 34, которая запрещает производство, распространение, импорт и использование аппаратного или программного обеспечения, специально предназначенного для облегчения совершения преступлений, перечисленных в ст. 27 – 33. Это включает трояны, кейлоггеры, боты и другие виды вредоносного программного обеспечения. При этом Закон Индонезии делает исключение для действий, направленных на исследование, тестирование систем или защиту информации при условии, что они осуществляются законно и добросовестно.

Опыт Саудовской Аравии позволяет выявить особый юридический подход к исследуемой проблематике. В отличие от законодательств, прямо криминализирующих создание и распространение вредоносного программного обеспечения как самостоятельный состав преступления, законодатель избрал иную стратегию, фокусируясь на пресечении конкретных противоправных действий, совершаемых с использованием таких компьютерных технологий.

Уголовно-правовая охрана за преступления в сфере ИКТ, содержится в Законе от 26.03.2007 № M/17«О борьбе с кибепреступностью» (далее – Закон Саудовской Аравии) [6]. Вредоносные программы в контексте данного закона рассматриваются прежде всего, как инструмент совершения киберпреступлений, а не как самостоятельный предмет общественно опасного посягательства.

Наиболее релевантными нормами, предусматривающими ответственность за действия с использованием вредоносных программ, выступают ст. 5 и 6 Закона Саудовской Аравии:

- статья 5 криминализирует несанкционированный доступ с намерением осуществить деструктивные действия (удаление, уничтожение, повреждение, изменение или несанкционированное распространение данных). Эти действия составляют сущность функционирования современных вредоносных программ, начиная от шифровальщиков-вымогателей и заканчивая деструктивными вирусами. Часть вторая данной статьи непосредственно наказывает за действия, приводящие к остановке или сбою работы информационной сети, что соответствует результатам деятельности DDoS-ботнетов и иных сетевых вредоносных программ. Часть третья, запрещающая воспрепятствование доступу к услугам и вызывание сбоев в их работе, также охватывает типичные последствия работы вредоносного программного обеспечения;

- статья 6 устанавливает ответственность за деяния, совершаемые с использованием компьютерных технологий, включая производство и распространение материалов, посягающих на общественную нравственность и религиозные ценности. Распространение подобного контента часто осуществляется через сети зараженных компьютеров (ботнеты), контролируемые с помощью вредоносных программ.

Важной процессуальной нормой является статья 13, предусматривающая конфискацию оборудования, программного обеспечения и иных средств, использованных при совершении киберпреступлений. Данное положение позволяет изымать как сами вредоносные программы, так и инструменты их создания и распространения.

Таким образом, законодатель, не криминализируя прямо создание и распространение вредоносных программ, создает эффективные правовые механизмы для борьбы с их использованием путем криминализации конкретных противоправных действий, совершаемых с их помощью.

Заключение

Проведенный анализ демонстрирует, что, несмотря на различия в правовых системах и подходах к криминализации, страны БРИКС последовательно развивают национальное законодательство в области противодействия киберпреступности, уделяя особое внимание борьбе с созданием, распространением и использованием вредоносных программ.

Наблюдается конвергенция правовых моделей, выражающаяся в дуалистическом подходе к квалификации вредоносных программ: как самостоятельного предмета преступного посягательства и как опасного инструмента для совершения других преступлений. В настоящее время, пожалуй, важным трендом является

криминализация не только непосредственного использования, но также создания и распространения вредоносных программ.

Полученные выводы свидетельствуют о необходимости дальнейшей гармонизации законодательств и укрепления международного сотрудничества в рамках БРИКС для создания единого правового пространства в сфере кибербезопасности, способного эффективно противостоять транснациональным киберугрозам.

Список литературы

1. Декларация Рио-Де-Жанейро от 06.07.2025, Бразилия. URL: http://static.kremlin.ru/media/events/files/ru/gvTArkWauqwuryk9xzLt3HuuI7EBmqrC.pdf (дата обращения: 26.08.2025).

2. Бегишев И.Р. Создание, использование и распространение вредоносных компьютерных программ // Проблемы права. 2012. № 3(34). С. 218-221. EDN PEWTKJ.

3. Иванова Л.В. Уголовно-правовое противодействие киберпреступности в странах БРИКС // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции (Долговские чтения): сборник материалов I Всероссийской науч.-практ. конф., Москва, 27 января 2021 г. / под общ. ред. О. С. Капинус ; науч. ред. В. В. Меркурьев, П. В. Агапов ; сост. М. В. Ульянов, Н. В. Сальников. Москва : Университет прокуратуры РФ, 2021. 460 с.

4. Мокофе У.М. Цифровые преобразования южноафриканского правового ландшафта // Journal of Digital Technologies and Law. 2023. № 1(4). С. 1087–1104.

5. Рогова Е.В. Уголовно-правовое противодействие киберпреступности в России и Китае: сравнительно-правовой аспект // Вестник Университета Прокуратуры Российской Федерации. 2024. № 1. С.84-90.

6. Anti-Cyber Crime Law (issued by Royal Decree No. M/17 in 8 Rabi'I 1428H (March 26, 2007)). URL: https://www.wipo.int/wipolex/en/text/498373 (дата обращения 26.08.2025).

7. Código Penal (Decreto-Lei № 2.848, de 7 de Dezembro de 1940). URL: https://www.planalto.gov.br/ccivil_03/decreto lei/del2848compilado.htm?utm_source (дата обращения 25.08.2025).

8. Computer Crime Proclamation No. 958/2016. July 7, 2016. URL: https://justice.gov.et/en/law/a-proclamation-to-provide-for-computer-crime/ (дата обращения 26.08.2025).

9. Criminal Law of the People's Republic of China. URL: http://www.chnlawyer.net/law/xingfa.pdf (дата обращения 25.08.2025)

10. Cybercrimes Act 19 of 2020. URL: https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf (дата обращения 25.08.2025).

11. Federal Decree-Law No. (34) of 2021 On Countering Rumors and Cybercrimes. URL: https://uaelegislation.gov.ae/en/legislations/1526 (дата обращения 26.08.2025).

12. Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law). URL: https://www.icnl.org/wp-content/uploads/Indonesia_elec.pdf (дата обращения 26.08.2025).

13. Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, Egypt. URL: https://www.wipo.int/wipolex/en/legislation/details/19959?utm_sourc%D0%B5 (дата обращения 25.08.2025).

14. Law No. 71063 on Computer Crimes. URL: https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=91715&utm_source (дата обращения 26.08.2025)

15. The Information Technology Act, 2000. URL: https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf (дата обращения: 25.08.2025).

УДК 343

Р. Э. Гильманов,
аспирант кафедры уголовного права и процесса,
преподаватель кафедры теории и истории государства и права,
Казанский инновационный университет
имени В. Г. Тимирясова

Виды роботов в современной правоприменительной практике и их использование в правоохранительной деятельности

Аннотация. В связи с активным использованием роботов и роботизированных систем, а также дронов в современных вооруженных силах, возникают вопросы, связанные с разрешением проблемы использования роботов в мирной жизни. Предлагается выделять самостоятельный тип правоохранительных роботов и роботизированных информационных технологий, а также начать разработку соответствующей нормативно-правовой регламентации их использования. Определяются основные варианты использования правоохранительных роботов, приводятся примеры практической реализации некоторых цифровых технологий, которые могут быть использованы при дальнейшем развитии технологий правоохранительных роботов.

Ключевые слова: робот, виды роботов, правоприменительная практика, правоохранительные роботы, цифровизация, дроны, «Безопасный город», правоохранительная деятельность

R.E. Gilmanov,
Postgraduate Student,
Lecturer at the Department of Theory and History of State and Law,
Kazan Innovative University named
after V. G. Timiryasov

Types of robots in modern law enforcement practice and their use in law enforcement activities

Abstract. Due to the active use of robots and robotic systems, as well as drones, in modern armed forces, there are issues related to the use of robots in civilian life. It is proposed to distinguish a separate type of law enforcement robots and robotic information technologies, as well as to begin developing appropriate legal regulations for their use. The main options for using law enforcement robots are identified, and examples of the practical implementation of certain digital technologies that can be used in the further development of law enforcement robot technologies are provided.

Keywords: robot, types of robots, law enforcement practice. law enforcement robots, digitalization, drones, Safe City, law enforcement activities

Введение. Цифровизация мира, создание цифровых экосистем, развитие цифрового пространства и автоматизация производств ведет современный мир к внедрению роботизированных систем, а также роботизированного труда. Одним из сопутствующих факторов, ведущих к внедрению роботов в повседневную жизнь, является использование в современных конфликтах дронов, при этом вариации их использования приобрели классовые различия и подразделяются на: одноразовые дроны FPV-UAV, дроны разведки (Reconnaissance & Surveillance UAV), Боевые дроны (Combat UAV), дроны-камикадзе (Loitering Munitions), также выделяют дроны радиоэлектронной борьбы и как отдельный подкласс – дроны логистики. При этом также во всем мире ведутся разработки роботов военного назначения, однако на современном этапе они не используются на регулярной основе, в перспективе они представляют угрозу [10]. К примеру, разработка компанией Boston Dynamics в 2005 по заказу управления перспективных разработок Министерства обороны США был разработан «4-х лапый» робот, и, хотя компания настаивала на исключительно гражданском применении своих разработок, у военных прослеживается высокая заинтересованность в дальнейшей милитаризации его использования.

В свете данных событий мы считаем необходимым рассмотреть понятие «робота», применительно к российскому законодательству, описать возможности их применения с гражданской точки зрения, и, как самостоятельной задачи, для обеспечения безопасности общества, что актуализирует задачу создания нового вида - правоохранительных роботов.

Основная часть. Понятие «робот» на данный момент не отражено в законодательстве, однако в научном сообществе уже предпринимаются попытки урегулировать данную сферу правоотношений. В частности, И.Р. Бегишевым был предложен проект Закона «Об обороте роботов, их составных частей (модулей)», в котором давалась следующая версия данного понятия: «робот – продукт достижений цифровых технологий (робототехническое устройство, комплекс, система), состоящий из двух или более составных частей (модулей), управляемый средствами заложенной в него компьютерной программы и способный как к выполнению заранее запрограммированных человеком действий, так и к автономному решению задач» [1; 2; 13; 14]. По нашему мнению, данное понятие является исчерпывающим.

Обращаясь к международному опыту регулирования вопроса робототехники, считаем необходимым упомянуть следующую практику.

В 2017 году Европарламентом была принята резолюция «Нормы гражданского права о робототехнике». В данной резолюции выделяются отличительные черты «умных роботов», заключающиеся в:

«- способности становится более автономными, используя сенсоры и/или обмениваясь информацией со своей средой (совместимость) и анализируя ее;

- способность обучаться на основе приобретенного опыта и в процессе взаимодействия;

- наличие формы физической поддержки робота;

- способность адаптировать свои действия и поведение в соответствии с условиями среды» [11].

В данной резолюции также выдвигается предложение о разделении роботов на подкатегории.

В Южной Корее был принят закон «О содействии развитию и распространению умных роботов». Где понятие «умный робот» обозначает «механическое устройство, которое способно воспринимать окружающую среду, распознавать обстоятельства, в которых оно функционирует, и целенаправленно передвигаться самостоятельно» [12].

Роботы приобретают все большее значение для государства, как с точки зрения экономики и быта, так и с социальной и культурной стороны [15]. Основными сферами использования роботов сейчас является промышленность, к примеру, роботы активно используются при сварочных работах и на сборочных конвейерах в автомобильной промышленности, в сельском хозяйстве, а также других видах производств [6]. Также перспективными представляется развитие роботизированных систем и самих роботов в быту и логистике, уже имеются роботы, осуществляющие функции по уборке, при строго установленном маршруте в рамках торговых центров [3]. Со стороны логистики – основным направлением является создание роботизированных конвейерных линий [8].

Одним из перспективных направлений развития роботов является их широкое распространение в сфере правоохранительных органов, особенно учитывая дефицит кадрового обеспечения. Представляется возможным оборудование уже имеющихся в Российской Федерации роботов Яндекс.Ровер, AGV 1811, либо же разработка совершенно новой технологии, подразумевающей под собой наличие специализированных функций для нужд по охране и обеспечению правопорядка.

Рассматривая далекие перспективы данной технологии, считаем необходимым упомянуть представление поп-культуры о технологиях, которые должны присутствовать в роботах данного типа, и сопоставление их с имеющимися на данный момент технологиями.

По нашему мнению, наиболее подходящее под цели правоохранительной деятельности представление о «правоохранительных роботах»» было сформировано в 2012 году, в игре «Call of Duty: Black ops II», одним из игровых концептов в которой был охранный робот A.S.R. (Automated Sentry Drone, что означает автоматический сторожевой дрон), целью которого было обеспечение безопасности в общественных зонах. Разработчиками игры, при создании данного вида роботов, в рамках игры, закладывались следующие функции – обеспечение безопасности определенной зоны,

устранение беспорядков, сопровождение и предоставление защиты для определенных лиц.

Функциональными особенностями данного робота являлись:

– наличие FPV-систем, которые уже активно применяются сегодня при конструировании дронов;

– использование, исходя из игровых особенностей, систем «машинного зрения»; современным аналогом, по нашему мнению, являются технологии LiDAR или Time-of-flight

– оружие летального и нелетального типа – роботы, использующие эти виды вооружения, уже анонсированы; к примеру, робот от компании Lobaev Robotix, PC1A3 Минирэкс, разработки Конструкторского Бюро Интегрированных Систем (КБИС) [9];

– использование для передвижения гусеничных систем передвижения, для обеспечения повышенной проходимости.

В настоящее время предложены некоторые виртуальные модели правоохранительных роботов, и не имеющих отношения к реальной жизни, однако наличие данного, «футуристичного», представления о деятельности правоохранительных органов, по нашему мнению, будет способствовать разработке необходимых технологий.

В то же время уже применяются отдельные правоохранительные роботы: 1) робот-полицейский Knightscope K5, который может патрулировать определенные территории, имеет функцию распознавания лиц, может сканировать номер автомобилей, фиксирует температуру окружающей среды и давление воздуха, может оповещать о подозрительной активности; 2) робот-патрульный AnBot, более скоростной (развивает скорость до 18 км/ч), распознает лица и может использовать электрошокер при задержании (полагаем, что здесь возможны правовые вопросы, связанные с правомерностью применения электрошокера), может фиксировать температуру и качество воздуха; 3) робот-помощник E-Parol Robot Sherif, который патрулирует железнодорожные станции, сканирует номера поездов и лица пассажиров; способен определять аномальную активность, включая дым, огонь, пожар.

Также нужно учитывать, что различные цифровые технологии уже активно применяются в правоохранительной деятельности. Так, в Москве с 2012 года работает интегрированная система видеонаблюдения, под контролем которой находятся практически все общественные места и крупные транспортные узлы. Используется данная система не только для фиксации совершаемых правонарушений и преступлений, но и для раскрытия ранее совершенных преступлений или поиска пропавших лиц, также для обеспечения общественной безопасности в ходе проведения массовых мероприятий.

Аналогичная система видеонаблюдения функционирует в Санкт-Петербурге, причем он имеется во всех районах города и включает сторонние системы видеонаблюдения, интегрированные в общую систему, например камеры

видеонаблюдения в аэропорту «Пулково», на железнодорожных вокзалах и в метрополитене.

В Казани активно используется система умного управления дорожным движением, а также развивается единая информационная система видеонаблюдения «Безопасный город», включающая 50 956 видеокамер. При этом функционал данной системы достаточно широкий: это моделирование сценариев потенциальных угроз для населения с предложением мер по их устранению; отслеживание статуса сообщений о разнообразных происшествиях (авариях, ДТП, несчастных случаях, правонарушениях и преступлениях); возможно использование в качестве инструмента для решения задач в сфере общественной безопасности (на уровне местных властей или выше); также возможно решение иных задач. В многоквартирных домах установлено более 19 тыс. IP-домофонов, что также повышает уровень общественной безопасности, и может осуществляться в автоматическом режиме. Однако тут могут возникнуть проблемы, связанные с раскрытием некоторых данных ввиду их утечки [4. С. 40].

Активно разворачивается система «Безопасный город» в Минеральных Водах, где уже подключено более 60 камер видеонаблюдения, и планируется подключение еще 36 камер в ближайшее время.

Системы «Безопасный город» или аналогичные присутствуют и в некоторых зарубежных странах. Так, в Индии в ряде городов (Дели, Мумби, Лакхнау, Калькутта, Ченнаи) запущена программа SaefCity («Безопсный город»), в которой участвует сеть видеокамер, включая расположенных в общественном транспорте, и в автоматическом режиме происходит считывание номерных знаков (систем ANPR). В Алжире видеокамеры используются для контроля над общественной безопасностью в наиболее крупных городах (городская система видеонаблюдения). В Саудовской Аравии системы камер видеонаблюдения позволяют контролировать потоки людей силам гражданской обороны.

Заметим, что страны БРИКС предполагают расширение взаимного сотрудничества в сфере городской и общественной безопасности, что также позволит развивать системы «Умных городов» в заинтересованных странах, и поставит вопрос о правовой помощи в виртуальном пространстве [5. С. 58].

Полагаем, что в дальнейшем информационные технологии, апробированные при создании и использовании технологии «Безопасный город» станут основой для работы правоохранительных роботов.

Заключение. Полагаем, что использование правоохранительных роботов имеет широкие перспективы и должно получить поддержку не только в правоохранительных органах, но и в правоприменительной практике и законодательной технике. Так, уже в настоящее время роботы и дроны могут быть использованы для патрулирования улиц и общественных мест, собирая информацию для дальнейшего анализа или для обнаружения подозрительных действий; в целях обеспечения общественной безопасности роботы могут быть использованы для сбора разведывательной

информации (тут необходимо четкое разграничение от вмешательства в частную жизнь [7. С. 43]); робот или дрон может использоваться для обнаружения так называемых «закладок» наркотических средств или психотропных веществ, взрывчатых веществ или иных запрещенных предметов; по налоги с военными роботами, их можно использовать для обезвреживания бомб или иных взрывоопасных предметов в мирной жизни (с учетом постоянно повышающейся террористической опасности); также есть направление использования роботов при тушении пожаров, спасении людей, перевозке грузов из / в опасные места; при осуществлении всех вышеперечисленных функций и задач робот может передавать видео- и звуковой сигнал, что облегчает управление им и дает дополнительную необходимую информацию.

Список литературы

1. Бегишев И. Р. Об обороте роботов, их составных частей (модулей) (инициативный проект федерального закона) : Препринт № 1 за 2021 г. / И. Р. Бегишев; Казанский инновационный университет им. В. Г. Тимирясова; Бегишев И. Р.. Казань : Издательство "Познание", 2021. 28 с. EDN FTFKAN.

2. Бегишев И. Р. Уголовно-правовое регулирование. Москва : Блок-Принт, 2022. 320 с. EDN GKMEDZ.

3. Бегишев И. Р. Технология искусственного интеллекта: мировой опыт развития // Baikal Research Journal. 2020. Т. 11, № 3. С. 1. EDN RWRYXO.

4. Гильманов Э.М., Гильманов Р.Э., Азаров Э.Е. Ответственность за раскрытие посредством сети Интернет данных, ставших известными в ходе проведения следственных действий / В сборнике: Цифровые технологии и право: Сборник научных трудов III Международной научно-практической конференции. В 6-ти томах. Казань, 20 сентября 2024 года / под ред. И.Р. Бегишева [и др.]. Том 3. Казань: Изд-во «Познание» Казанского инновационного ун-та, 2024. С. 39-41.

5. Гончарова Н. Н. Правовая помощь в виртуальном пространстве // Цифровые технологии и право : Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года / Под редакцией И.Р. Бегишева [и др.]. Том 2. Казань: Издательство "Познание", 2022. С. 57-59. EDN XCEBUN.

6. Какие роботы применяются в отраслях промышленного производства // ФРУКТОНАД URL: https://sixdof.ru/kakie-roboty-primenyajutsya-v-otraslyah-promyshlennogo-proizvodstva/ (дата обращения: 09.09.2025).

7. Латыпова Э.Ю. Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Oeconomia et Jus. 2019. № 2. С. 35-45.

8. Роботы по отраслям и назначению (области применения роботов) // RoboTrends URL: https://robotrends.ru/robopedia/roboty-po-otraslyam-i-naznacheniyu (дата обращения: 09.09.2025).

9. Тактический мобильный робот РС1А3 Минирэкс // Большая Военная Энциклопедия URL: https://zonwar.ru/news/news_164_RS1A3.html (дата обращения: 09.09.2025).

10. Humans and Robots: Transformations of Professional Communication in the Digital Era / I. Begishev, A. Shutova, D. Niyozmetov [et al.] // 2025 Communication Strategies in Digital Society Seminar (ComSDS), Saint Petersburg, Russian Federation, 09 апреля 2025 года. Vol. 2025. IEEE: IEEE, 2025. P. 144-148. DOI 10.1109/ComSDS65569.2025.10971289. EDN PTSCQC.

11. Нормы гражданского права о робототехнике. P8_TA_PROV(2017)0051 Европарламент [Электронный ресурс] https://robotrends.ru/images/1725/66137/201706722_Resolution_and_Charter_EU_RoboTrendsru.pdf (дата обращения: 09.09.2025).

12. Регулирование робототехники в Корее. Закон о содействии развитию и распространению умных роботов [Электронный ресурс] https://robotrends.ru/pub/1730/regulirovanie-robototehniki-v-koree.-zakon-o-sodyaystvii-razvitiyu-i-rasprostraneniyu-umnyh-robotov (дата обращения: 09.09.2025).

13. Бегишев И. Р. Цифровая терминология: подходы к определению понятия "робот" и "робототехника" // Информационное общество. 2021. № 2. С. 53-66. EDN TKAAMV.

14. Бегишев И. Р. Искусственный интеллект и робототехника : глоссарий понятий / И. Р. Бегишев, З. И. Хисамова. – Москва : Общество с ограниченной ответственностью «Проспект», 2021. 64 с. EDN HQELSK.

15. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185-201. EDN TBUVGY.

УДК 343.140.02

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

Цифровые доказательства в уголовном процессе: границы допустимости и проблемы фальсификации

Аннотация. В статье рассматриваются вопросы правовой природы цифровых доказательств в уголовном праве и процессе. Особое внимание уделяется определению их допустимости в уголовном деле, а также проблемам, связанным с возможностью фальсификации электронных данных. Анализируются основные виды цифровых доказательств: электронные документы, фото-, аудио- и видеоматериалы, метаданные, данные транзакций и устройств. Показано, что в условиях цифровизации наибольшую актуальность приобретают проблемы достоверности и сохранности электронных данных, а также обеспечение «цепочки хранения». Авторы обосновывают необходимость комплексного подхода, включающего как правовое регулирование, так и внедрение технических средств защиты.

Ключевые слова: цифровые доказательства, допустимость доказательств, фальсификация доказательств, судебная экспертиза, цифровизация, метаданные

E. M. Gilmanov,
Senior Lecturer at the Department of Criminal Law and Procedure,
Kazan Innovative University named after V.G. Timiryasov,
E. E. Azarov,
student,
Kazan Innovative University named after V.G. Timiryasov

Digital evidence in criminal procedure: limits of admissibility and problems of falsification

Abstract. The article discusses the issues of the legal nature of digital evidence in criminal law and the process. Special attention is paid to determining their admissibility in a criminal case, as well as problems related to the possibility of falsification of electronic data. The main types of digital evidence are analyzed: electronic documents, photo, audio and video materials, metadata, transaction and device data. It is shown that in the context of digitalization, the problems of reliability and safety of electronic data, as well as ensuring the

«storage chain», are becoming the most urgent. The authors substantiate the need for an integrated approach, including both legal regulation and the introduction of technical means of protection.

Keywords: digital evidence, admissibility of evidence, falsification of evidence, forensic examination, digitalization, metadata

Введение. Цифровизация затронула все сферы общественных начал и реалий жизни, также внесла коррективы в некогда привычные процессы уголовного судопроизводства. Сегодня мы неоспоримо говорим о том, что значительная часть информации, которая имеет определяющее значение для расследования преступлений и последующего всестороннего судебного разбирательства, существует в цифровом виде. Письма, созданные и направленные средствами моментальной доставки до адресата в рамках информационных технологий, «диалоги» между пользователями средств электронного социального взаимодействия, информационные «посты» в мессенджерах, данные геолокации, цифровые фотографии и видеозаписи, сведения с электронных устройств, с каждым днем становятся неотъемлемой частью жизни каждого индивида, участвующего в общественных отношениях, а равно могут и должны рассматриваться как доказательства при расследовании преступлений.

Однако специфика цифровой среды порождает новые вызовы, требующие незамедлительного и обоснованного ответа. В отличие от доказательств, которые существовали исключительно на бумажных носителях, цифровые данные, как мы можем свидетельствовать, подвергаются изменению и, вследствие, их фальсификации. Кроме того, остается открытым вопрос о границах допустимости приобщения цифровых доказательств и их использования в уголовном процессе; нет ясности, что именно может быть признано доказательством; каким образом проходит проверка достоверности источника; каким образом обеспечить сохранность цифровых данных от вмешательств из вне.

Основная часть. В российском уголовно-процессуальном законодательстве закреплено, что доказательствами по уголовному делу могут быть любые сведения, имеющие значение для установления обстоятельств дела (ст. 74 УПК РФ). В связи с фундаментальным изменением средств обращения и обмена данными, которые по сей день протекают в Российской Федерации, при расследовании преступлений уполномоченные на истребование и приобщение доказательств лица стали включать в материалы уголовного дела цифровые доказательства. Как мы понимаем, это данные, представленные в электронном виде на различных носителях информации, извлеченные, сохраненные и представленные в установленном законом порядке, которые могут быть использованы для установления обстоятельств уголовного дела. Вместе с тем, отметим важность сохранения тайны следствия, которая включает ряд взаимосвязанных ситуаций, направленных на наиболее полное раскрытие и расследование преступления [3. С. 40]. К сожалению, наблюдаются и процессы

случайного или преднамеренного раскрытия тайны следствия, особенно цифровых данных, посредством средств массовой информации или через социальные сети [2. С. 109].

Таким образом, мы приходим к анализу основных видов цифровых доказательств, к которым относятся электронные документы, представленные в виде переписки по электронной почте, сообщения мессенджеров, электронные файлы, передаваемые и сохраняемые на различных носителях, а равно фото-, аудио- и видеоматериалы, изъятые или сохраненные с различного рода устройств. Также отметим довольно спорную, но неотъемлемую часть электронных данных, которая именуется метаданными, представленными в виде даты и времени создания файла, IP-адреса, геолокационных данных и сведений иного рода. Данные устройств IoT (Internet of Things) смарт-часов, фитнес-браслетов, домашних камер и сенсоров, призванных проводить мониторинг окружающей среды с помощью различных датчиков, а ткже системы умных домов (smathouse) [1. С. 169]. Главное отличие цифровых доказательств от традиционных состоит в их высокой зависимости от технических средств фиксации и хранения, а также в сложности проверки их подлинности без специализированных знаний и оборудования, а также с появлением и внедрением новейшего высокотехнологичного оборудования и возможностями использования искусственного интеллекта [9. С. 136]. Также могут возникать проблемы, связные с получением копий процессуальных документов, если они существуют в цифровой форме [8. С. 346].

В данном ключе мы говорим о допустимости доказательств, которая определяется их законностью, относимостью и достоверностью. Для цифровых доказательств эта проблема, как мы полагаем, представлена особенно остро. Особое значение приобретает также проблема «цепочки хранения» (chain of custody) фиксации каждого этапа обращения с цифровыми доказательствами. Любое нарушение этой цепочки ставит под сомнение подлинность данных. В мире цифровых технологий любая информация может облететь мир за считанные секунды, однако, в случае распространения ложной информации, последствия такого информирования трудно спрогнозировать [6. С. 36-37; 7. С с. 149]. Соответственно, как правильно отмечается Э.М. Гильмановым и Д.В. Кирпичниковым, необходимо разрабатывать методики расследования преступлений в сфере обращения цифровой информации [4. С. 275] и ее использования. Также правильное и рациональное использование цифровых технологий позволяет значительно сократить материальные затраты на досудебных и судебных стадиях уголовного процесса [5. С. 133], что можно рассматривать с разных позиций – и как возможность их использования для сохранения цифровых доказательств, так и для сокращения стадии дознания и предварительного расследования, путем избежания дополнительных следственных действий и т.п. Нужно учитывать и тот факт, что современные технологии существенно облегчают процесс изменения электронных данных в противоправных интересах лиц, желающих избежать

наказания, либо использующих возможность фальсификации для реализации аморальных или иных низменных мотивов.

Заключение. Цифровые доказательства становятся неотъемлемой частью уголовного процесса, однако их использование сопряжено с серьезными и обоснованными рисками. Мы рассмотрели основные проблемы в контексте, связанном с возможностью их фальсификации, и с трудностями обеспечения их достоверности. Оптимальным решением, как нам представляется, является разработка единого правового стандарта цифровых доказательств, включающего: закрепление процедур извлечения, хранения и проверки цифровых доказательств; обязательность судебной экспертизы цифровых данных; использование современных технологий защиты (блокчейн, цифровая подпись, защищенные хранилища для электронных файлов). Поэтому стоит особо отметить авторские концепции электронного доказательства [10. С. 288].

Таким образом, только при условии гармоничного сочетания правовых и технических гарантий цифровые доказательства смогут выполнять свою функцию в уголовном процессе без угрозы нарушения прав личности и принципов справедливого судопроизводства.

Список литературы

1. Гильманов Р.Э. Криминологические риски использования умных домов (smarthouse) / В сборнике: «Молодой исследователь: актуальные проблемы, достижения и инновации: сборник тезисов XXVII региональной студенческой научно-практической конференции (г. Набережные Челны, 29 марта 2024 г.). Казань: Изд-во «Познание» Казанского инновационного ун-та, 2024. С. 169.

2. Гильманов Р.Э., Азаров Э.Е. СМИ как инструмент влияния на общественно мнение и ответственность за его использование / В сборнике: Цифровые технологии и право: Сборник научных трудов III Международной научно-практической конференции. В 6-ти томах. Казань, 20 сентября 2024 года / под ред. И.Р. Бегишева [и др.]. Том 4. Казань: Изд-во «Познание» Казанского инновационного ун-та, 2024. С. 107-111.

3. Гильманов Э.М., Гильманов Р.Э., Азаров Э.Е. Ответственность за раскрытие посредством сети Интернет данных, ставших известными в ходе проведения следственных действий / В сборнике: Цифровые технологии и право: Сборник научных трудов III Международной научно-практической конференции. В 6-ти томах. Казань, 20 сентября 2024 года / под ред. И.Р. Бегишева [и др.]. Том 3. Казань: Изд-во «Познание» Казанского инновационного ун-та, 2024. С. 39-41.

4. Гильманов Э.М., Кирпичников Д.В. О необходимости разработки методики расследования преступлений в сфере обращения цифровой информации // Актуальные проблемы государства и права. 2020. Т. 4. № 14. С. 262-277.

5. Закирова Э.Ф., Шайхутдинова З.З. Тенденция сокращения материальных затрат на досудебных и судебных стадиях уголовного процесса / В сборнике: Обеспечение прав участников в досудебных стадиях уголовного судопроизводства. Материалы Всероссийской научно-практической конференции. Кубанский государственный университет. Краснодар, 2025. С. 129-135.

6. Латыпова Э.Ю., Гильманов Р.Э. Уголовно-правовая ответственность за распространение фейков в социальных сетях / В сборнике: Цифровые технологии и право: Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года / под ред. И.Р. Бегишева [и др.]. Том 5. Казань: Изд-во «Познание» Казанского инновационного ун-та, 2023. С. 36-39.

7. 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 28 апреля 2022 года. – В 3-х т. – Т.1: Секция 1: Актуальные проблемы современного права и управления: теория и практика. – ГОУ ВПО «Донбасская юридическая академия» / отв. ред.: Е.В. Ковтун. – Донецк: «Цифровая типография», 2022. – 338 с. – С. 147-153.

8. Латыпова Э.Ю., Гильманов Э.М., Кирпичников Д.В. Роль прокурора в обеспечении права потерпевшего на получение копий процессуальных документов / В сборнике: 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.]. 2020. С. 339-347.

9. Латыпова Э.Ю., Мусина Р.Р., Гильманов Э.М. Цифровые технологии в расследовании экономических преступлений / В сборнике: Цифровые технологии и право: Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года / под ред. И.Р. Бегишева [и др.]. Том 2. Казань: Издательство "Познание", 2022. С. 135-139.

10. Дмитриева А.А., Пастухов П.С. Понятие электронных доказательств в уголовном судопроизводстве // Журнал цифровых технологий и права. 2023. Т. 1, № 1. С. 270-295. https://doi.org/10.21202/jdtl.2023.11. EDN: SGAOKS.

УДК 343.91

Ю. М. Графова,
соискатель,
Казанский инновационный университет
имени В. Г. Тимирясова

Особенности личности преступника, совершающего мошенничество с использованием социальной инженерии

Аннотация. Настоящая статья посвящена криминологическому анализу личностных характеристик субъектов преступлений, совершающих мошеннические действия с использованием методов социальной инженерии. В работе рассматриваются психологические детерминанты противоправного поведения, включающие когнитивные особенности, мотивационную структуру, эмоционально-волевые качества и социально-психологические характеристики лиц, избирающих данный способ совершения общественно опасных деяний. Автором предпринята попытка систематизации типологических групп преступников через призму дифференцированного подхода к анализу криминогенной личности в контексте современных форм киберпреступности. Особое внимание уделяется механизму формирования антиобщественной направленности личности и роли социально-психологических факторов в генезисе преступного поведения. Исследование базируется на анализе материалов уголовных дел и результатов психологического обследования осужденных лиц. Полученные результаты могут быть использованы для совершенствования методов расследования данной категории преступлений и разработки мер индивидуальной профилактики.

Ключевые слова: социальная инженерия, личность преступника, мошенничество, криминогенные факторы, антиобщественная направленность, психологический портрет, киберпреступность, манипулятивное поведение, криминальная мотивация, профилактика преступлений

Yu. M. Grafova,
graduate student,
Kazan Innovative University
named after V. G. Timiryasov

Characteristics of the criminal's personality, committing fraud using social engineering

Abstract. This article is devoted to the criminological analysis of the personal characteristics of the subjects of crimes who commit fraudulent acts using social engineering methods. The paper examines the psychological determinants of illegal behavior, including cognitive features, motivational structure, emotional and volitional qualities, and socio-

psychological characteristics of individuals who choose this method of committing socially dangerous acts. The author attempts to systematize typological groups of criminals through the prism of a differentiated approach to the analysis of criminogenic personality in the context of modern forms of cybercrime. Special attention is paid to the mechanism of formation of antisocial personality orientation and the role of socio-psychological factors in the genesis of criminal behavior. The study is based on the analysis of materials from criminal cases and the results of psychological examinations of convicted persons. The results obtained can be used to improve the methods of investigation of this category of crimes and the development of individual prevention measures.

Keywords: social engineering, criminal identity, fraud, criminogenic factors, antisocial orientation, psychological profile, cybercrime, manipulative behavior, criminal motivation, crime prevention

Введение

В свете перехода от информационного общества к цифровому значительное внимание уделяется цифровым технологиям и процессам, происходящим с ними [1. С. 123]. Трансформация современного общества под влиянием процессов цифровизации обусловила появление качественно новых форм преступного поведения, характеризующихся высокой степенью латентности и специфическими способами воздействия на потерпевших [2]. Мошенничество с использованием социальной инженерии представляет собой особую разновидность корыстных посягательств, отличающуюся сложным механизмом совершения и требующую от субъекта преступления обладания специфическими личностными качествами и профессиональными навыками.

Криминологическое значение исследования личности преступника, специализирующегося на данном виде противоправной деятельности, обусловлено необходимостью выявления закономерностей формирования антиобщественной направленности личности в условиях информационного общества и разработки эффективных мер индивидуального предупреждения преступлений [3]. Понимание психологических механизмов, лежащих в основе выбора способа совершения преступления, создает методологическую базу для совершенствования тактики расследования и повышения эффективности профилактического воздействия на лиц, склонных к совершению подобных деяний [4].

Актуальность проблематики подтверждается устойчивой тенденцией роста регистрируемых фактов мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий [5], что свидетельствует о формировании устойчивой криминальной специализации значительного числа правонарушителей в данной сфере.

Основная часть

Теоретико-методологические основы криминологического анализа личности преступника

Методологический подход к исследованию личности преступника, совершающего мошенничество с использованием социальной инженерии, базируется на фундаментальных положениях криминологической науки о детерминации преступного поведения и роли личностных факторов в механизме совершения преступления. Концептуальную основу анализа составляет учение о криминогенной личности как носителе причин преступного поведения, характеризующейся специфической совокупностью социально-психологических свойств и качеств.

В контексте рассматриваемой проблематики особую значимость приобретает категория антиобщественной направленности личности, понимаемой как устойчивая система взглядов, установок и ценностных ориентаций, детерминирующих выбор преступного способа удовлетворения потребностей и разрешения жизненных противоречий. Применительно к субъектам мошенничества с использованием социальной инженерии антиобщественная направленность проявляется в форме пренебрежительного отношения к правам и интересам других лиц, готовности к использованию обмана и злоупотребления доверием как основных способов достижения корыстных целей.

Структурный анализ личности преступника предполагает рассмотрение биологических, психологических и социальных детерминант противоправного поведения в их системном единстве и взаимообусловленности. Биологический компонент включает нейрофизиологические особенности, влияющие на способность к манипулятивному воздействию и эмоциональной регуляции поведения. Психологический уровень характеризуется когнитивными способностями, мотивационной структурой и эмоционально-волевыми качествами. Социальный аспект охватывает статусно-ролевые характеристики, особенности социализации и микросоциальной среды.

Социально-демографические характеристики субъектов преступлений

Эмпирический анализ уголовно-статистических данных и материалов судебно-следственной практики позволяет выделить типичные социально-демографические характеристики лиц, совершающих мошенничество с использованием социальной инженерии. Возрастная структура данной категории преступников характеризуется преобладанием лиц молодого и среднего возраста (25-40 лет), что обусловлено необходимостью обладания достаточным уровнем компьютерной грамотности и знанием современных информационных технологий.

Образовательный уровень субъектов рассматриваемых преступлений значительно превышает среднестатистические показатели по преступности в целом. Большинство правонарушителей имеют высшее или среднее специальное образование, часто в сфере информационных технологий, экономики, психологии или юриспруденции. Данная особенность объясняется спецификой способов совершения преступления, требующих глубокого понимания психологических механизмов воздействия на потерпевших и знания правовых аспектов финансовой деятельности.

Профессиональная принадлежность характеризуется разнообразием сфер деятельности, однако отмечается повышенная концентрация лиц, имеющих опыт работы в области информационных технологий, телекоммуникаций, банковской сферы, а также в сфере продаж и маркетинга. Указанная закономерность обусловлена наличием профессиональных навыков, востребованных при совершении мошеннических действий с использованием социальной инженерии.

Гендерное распределение характеризуется значительным преобладанием мужчин (около 70%), что соответствует общим тенденциям корыстной преступности. Однако отмечается возрастание доли женщин среди субъектов данных преступлений, что связано со спецификой способов воздействия, не требующих применения физической силы и позволяющих эксплуатировать гендерные стереотипы при установлении психологического контакта с потерпевшими.

Психологические особенности личности преступника

Психологический портрет субъекта мошенничества с использованием социальной инженерии характеризуется комплексом специфических когнитивных, эмоционально-волевых и коммуникативных особенностей, обеспечивающих эффективность манипулятивного воздействия на потерпевших. К числу основных психологических детерминант следует отнести высокий уровень интеллектуального развития, развитые коммуникативные способности, эмоциональную устойчивость в стрессовых ситуациях, а также способность к быстрой адаптации и принятию решений в изменяющихся условиях.

Интеллектуальные способности проявляются в форме аналитического мышления, позволяющего анализировать психологические особенности потенциальных жертв, прогнозировать их поведенческие реакции и разрабатывать эффективные стратегии воздействия. Креативность мышления обеспечивает способность к генерированию нестандартных решений и адаптации известных схем мошенничества к конкретным ситуациям. Развитая память и внимание позволяют удерживать в сознании множество деталей легенды и своевременно реагировать на изменения в поведении потерпевшего.

Коммуникативные способности включают владение техниками вербального и невербального воздействия, умение устанавливать психологический контакт с различными категориями граждан, способность к эмпатии и эмоциональному заражению. Особое значение имеет развитость навыков активного слушания, позволяющих быстро выявлять психологические особенности собеседника и адаптировать тактику воздействия к его индивидуальным характеристикам.

Эмоционально-волевая сфера характеризуется высоким уровнем самоконтроля, способностью к длительному поддержанию заданного эмоционального состояния, стрессоустойчивостью и готовностью к риску. Данные качества обеспечивают возможность успешного исполнения различных социальных ролей в процессе

реализации мошеннических схем и сохранения психологической устойчивости при возникновении непредвиденных обстоятельств.

Мотивационная структура преступного поведения

Анализ мотивационной сферы субъектов мошенничества с использованием социальной инженерии выявляет сложную иерархическую структуру побуждений, включающую как непосредственные корыстные мотивы, так и более глубокие психологические потребности, удовлетворение которых достигается посредством совершения преступных действий. Корыстная мотивация, традиционно рассматриваемая в качестве доминирующего фактора при совершении имущественных преступлений, в данном случае часто осложняется дополнительными мотивационными компонентами.

Ведущую роль в мотивационной структуре играет стремление к материальному обогащению, однако специфика способа совершения преступления обусловливает актуализацию потребностей в самоутверждении, социальном признании и демонстрации интеллектуального превосходства. Процесс разработки и реализации сложных мошеннических схем нередко воспринимается субъектом как интеллектуальная игра, позволяющая продемонстрировать собственную изобретательность и превосходство над потерпевшими и правоохранительными органами.

Значительную роль в формировании мотивации играет потребность во власти и контроле над другими людьми, реализуемая посредством манипулятивного воздействия и принуждения к совершению действий в интересах преступника. Данная потребность часто коррелирует с нарциссическими чертами личности и завышенной самооценкой, характерной для значительной части субъектов рассматриваемых преступлений.

Дополнительным мотивационным фактором выступает стремление к избежанию социальной ответственности и получению «легких денег» без затрат физических усилий и времени, необходимых для законного заработка. Данная мотивация особенно характерна для лиц с выраженными гедонистическими установками и низким уровнем социальной ответственности.

Нравственно-психологические особенности криминогенной личности

Нравственно-психологический облик субъекта мошенничества с использованием социальной инженерии характеризуется деформацией ценностно-нормативной системы личности, проявляющейся в искаженном восприятии морально-этических категорий и готовности к нарушению общепринятых норм социального поведения. Основными индикаторами нравственной деформации выступают цинизм в отношении к потерпевшим, рационализация противоправного поведения и отсутствие чувства вины за причиненный ущерб.

Циничное отношение к потерпевшим проявляется в восприятии их в качестве объектов для извлечения материальной выгоды, лишенных субъектности и права на защиту своих интересов. Характерной особенностью является способность к эмоциональному отстранению от страданий жертв и рассмотрению причиненного

ущерба исключительно в инструментальном аспекте как средства достижения поставленных целей.

Рационализация противоправного поведения осуществляется посредством использования различных психологических механизмов защиты, включающих минимизацию общественной опасности совершаемых деяний, перекладывание ответственности на потерпевших («сами виноваты в своей доверчивости»), а также идеологическое оправдание преступной деятельности через призму социального неравенства и несправедливого распределения материальных благ.

Отсутствие чувства вины и раскаяния обусловлено как нарциссическими особенностями личности, так и специфическими когнитивными искажениями, препятствующими адекватной оценке морально-этических аспектов совершаемых деяний. Данная особенность создает существенные препятствия для ресоциализации и исправления осужденных, требуя применения специальных методов психологического воздействия.

Типология личности преступников

На основании проведенного анализа личностных характеристик субъектов мошенничества с использованием социальной инженерии представляется возможным выделить несколько основных типологических групп, различающихся по доминирующим мотивационным факторам, способам организации преступной деятельности и психологическим особенностям.

Первый тип – «интеллектуальный манипулятор» – характеризуется высоким уровнем образования и интеллектуального развития, склонностью к тщательному планированию преступных действий и использованию сложных многоэтапных схем воздействия на потерпевших. Представители данной группы часто имеют опыт работы в сферах, требующих аналитических способностей и знания человеческой психологии. Мотивационная структура характеризуется сочетанием корыстных побуждений с потребностью в интеллектуальном самоутверждении.

Второй тип – «социальный актер» – отличается развитыми коммуникативными способностями, артистическими данными и способностью к перевоплощению в различные социальные роли. Данная категория преступников специализируется на непосредственном взаимодействии с потерпевшими и использовании эмоционального воздействия для достижения поставленных целей. Характерными особенностями являются экстравертированность, эмоциональная лабильность и выраженная потребность во внимании окружающих.

Третий тип – «технический специалист» – представлен лицами с глубокими знаниями в области информационных технологий, специализирующимися на технической стороне реализации мошеннических схем. Психологические особенности включают интровертированность, склонность к системному мышлению и предпочтение опосредованных форм взаимодействия с потерпевшими через технические средства связи.

Четвертый тип – «организатор преступной деятельности» – характеризуется лидерскими качествами, способностью к координации действий соучастников и стратегическому планированию преступной деятельности. Представители данной группы часто выступают в качестве руководителей организованных преступных групп и редко принимают непосредственное участие в контактах с потерпевшими, сосредотачиваясь на организационных аспектах противоправной деятельности.

Заключение

Проведенное исследование особенностей личности преступника, совершающего мошенничество с использованием социальной инженерии, позволяет сформулировать ряд принципиальных выводов относительно психологических детерминант данного вида противоправного поведения и механизмов формирования специализированной преступной деятельности в сфере киберпреступности.

Установлено, что субъекты рассматриваемых преступлений характеризуются специфическим комплексом личностных особенностей, включающим высокий интеллектуальный потенциал, развитые коммуникативные способности, деформированную нравственно-ценностную систему и сложную мотивационную структуру, сочетающую корыстные побуждения с потребностями в самоутверждении и социальном признании.

Полученные результаты имеют существенное практическое значение для совершенствования методов расследования данной категории преступлений, разработки эффективных тактических приемов изобличения виновных лиц и формирования научно обоснованной системы индивидуального предупреждения рецидивных проявлений противоправного поведения.

Список литературы

1. Шутова А. А. Понятие, система и признаки цифровых преступлений // Правопорядок: история, теория, практика. 2024. № 4(43). С. 122-128. DOI 10.47475/2311-696X-2024-43-4-122-128.

2. Аувал А. М. Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности / А. М. Аувал, С. Лазарус // Journal of Digital Technologies and Law. 2024. Т. 2, № 4. С. 915-942. EDN JVGLRH.

3. Майоров А. В. Влияет ли цифровизации на виктимизацию в современном обществе? // Виктимология. 2022. Т. 9, № 2. С. 148-156. EDN MLRFKH.

4. Бегишев И. Р. Отзыв на автореферат диссертации Зотиной Елены Владимировны на тему: «Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование» // Социальное управление. 2025. Т. 7, № 2. С. 72-76. EDN GPURSQ.

5. Бегишев И. Р. Создание, использование и распространение вредоносных компьютерных программ // Проблемы права. – 2012. – № 3(34). – С. 218-221. – EDN PEWTKJ.

УДК 34.488

В. В. Денисович,
кандидат юридических наук, доцент,
старший научный сотрудник,
Казанский инновационный университет
имени В. Г. Тимирясова

Криминальные риски, связанные с применением и использованием метавселенных

Аннотация. Исследование основано на доктринально-правовом подходе, который позволил провести системный анализ правового поля в сфере метавселенных: эволюция понятия метапреступность и метапреступление, применимость термина метапреступность в современной криминологии, ответственность за метапреступления. Автор отмечает, что метапреступность своими корнями уходит в социальную теорию происхождения преступности. Рассматриваются формы взаимодействия правоохранительных органов Российской Федерации и международных организаций по профилактике и предупреждению распространения метапреступлений. Автор анализирует признаки метаприступности и отличительные особенности данного вида преступности в сравнении с киберпреступностью. Особое внимание уделяется перспективному изучению метапреступности в будущем и формировании концепта метапреступлений в теории уголовного права и криминологии.

Ключевые слова: метапреступность, виртуальные преступления, метапреступления, правовое регулирование виртуальных пространств, аватар

V. V. Denisovich
Candidate of Law, Associate Professor, Senior Researcher Research,
Kazan Innovative University named
after V. G. Timiryasov

Criminal risks associated with the application and use of metaverse

Abstract. The study is based on a doctrinal and legal approach, which allowed for a systematic analysis of the legal field in the field of metaverses: the evolution of the concept of meta-crime and meta-offense, the applicability of the term meta-crime in modern criminology, and the responsibility for meta-crimes. The author notes that meta-crime has its roots in the social theory of the origin of crime. The study examines the forms of cooperation between law enforcement agencies of the Russian Federation and international organizations in the prevention and control of the spread of meta-crimes. The author analyzes the characteristics of meta-crime and its distinctive features in comparison with cybercrime.

Keywords: meta-crime, virtual crimes, meta-crimes, legal regulation of virtual spaces, avatar

Введение. С целью скрупулезного исследования термина метавселенная в поле зрения уголовного закона представляется интересным обратится к следующим ключевым исследованиям как отраслевого, так и межотраслевого характера.

Термин «метавселенная» («Metaverse») впервые был использован Н. Стивенсоном в романе 1992 г. «Лавина» («Snow Crash»), где метавселенная представлена как постоянно действующий виртуальный мир, в котором люди взаимодействуют через свои аватары («avatar»)[3]. Само слово «метавселенная» образовано от английского «meta»[4] – «трансцендентность» и «verse» - «мир». Под метавселенной понимают коллективное виртуальное пространство, в котором объединяются физическая, дополненная (смешанная или гибридная реальность) и виртуальная реальность и гаптика[5]. Определение метавселенной, выработанное М. Боллом, звучит следующим образом: «Это масштабируемая и совместимая сеть визуализируемых в реальном времени 3D-виртуальных миров и сред, которые могут синхронно и постоянно восприниматься практически неограниченным числом пользователей с индивидуальным ощущением присутствия и непрерывностью данных, таких как личность, история, права, объекты, коммуникации и платежи»[6]. Т.Я. Хабриева отмечает: «Цифровые технологии способны менять образ права, влиять на его регулятивный потенциал и эффективность, открывать дорогу или блокировать его действие в новых измерениях социальной реальности»[7].

Четкого определения метавселенных не выработано ни одной отраслью права[8], именно эту задачу следует решить в рамках представленного исследования. Однако следует оговориться, с целью не нарушить правила научного методологического

---

[3] «Индивидуальный цифровой идентификатор личности (цифровой аватар)» в Модельном законе о цифровых правах (приложение к Постановлению Межпарламентской Ассамблеи государств – участников СНГ от 14 апреля 2023 г. N 55-12) определен как «набор символов, изображение или иное условное обозначение, позволяющее идентифицировать в информационной системе субъекта, у которого возникают субъективные гражданские права и обязанности при использовании цифрового аватара в информационной системе». Johnson D.R., Post D.G. Law and Borders - The Rise of Law in Cyberspace // Stanford Law Review. 1996. Vol. 48. P. 1367 - 1402.

[4] Деятельность Meta Platforms Inc. по реализации продуктов - социальных сетей Facebook и Instagram на территории РФ запрещена по основаниям осуществления экстремистской деятельности.

[5] Wang Y., Su Z., Zhang N. [et al.]. A Survey on Metaverse: Fundamentals, Security, and Privacy // arXiv:2203.02662v4.

[6] Ball M. What It Is, Where to Find it, and Who Will Build It. 13.01.2020. URL: https://www.matthewball.vc/all/themetaverse.

[7] Хабриева Т.Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. N 9. С. 15.

[8] См., например: Лескина Э.И. Метавселенная и задачи в области правового регулирования данных // Юрист. 2023. N 3; Овчинников А.И., Ширинских П.И. Метавселенные и право: вызовы новых технологий в условиях дальнейшего развития Интернета // Вестник юридического факультета Южного федерального университета. 2023. Т. 10. N 2.

подхода при покрытии предметной области концепта и определить в качестве основной задачи – определение метавселенной в рамках данного работы, как объекта именно уголовно-правовой охраны.

Итак, метавселенная многими авторами описывается как новая итерация интернета, которая использует гарнитуры виртуальной реальности, технологию блокчейн и аватары в рамках новой интеграции физического и виртуального миров[9]. Существует две позиции, которые противоречат друг другу: 1) метавселенные заменят Интернет; 2) метасреда является квазиправопреемницей мобильного Интернета, преобразовывает его[10].

Современная правовая система переживает значительные трансформации, среди которых особенно выделяется активное внедрение цифровых технологий в повседневную жизнь граждан. Важным этапом на этом пути стало окончательное утверждение и последующее официальное опубликование Цифрового кодекса Российской Федерации, что свидетельствует о формировании новой парадигмы правового регулирования в цифровую эпоху. Параллельно с этим наблюдается тенденция к применению кодексов профессиональной этики в контексте цифрового законодательства, которая стала возможной благодаря стремительному развитию информационных технологий.

Процесс формирования нового правового пространства Российской Федерации происходит в условиях растущих социальных потребностей в цифровизации, что требует адекватного нормативного закрепления. Этот процесс характеризуется высокой динамикой, однако о полной кодификации цифрового законодательства говорить пока преждевременно. Также следует отметить, что на доктринальном уровне еще не сформированы базовые терминологические категории, необходимые для создания полноценной нормативной правовой базы в сфере цифрового права. Это подчеркивает высокую актуальность и значимость исследования данной темы.

Ключевая детерминанта метапреступности заключается в формировании новых парадигм криминального взаимодействия. В условиях цифровизации общества, цифровые платформы, защищенные мессенджеры и анонимные сети (даркнет) создают технологическую инфраструктуру для возникновения распределенных преступных сетей, функционирующих на принципах децентрализации. В отличие от традиционных организованных преступных структур с жесткой иерархией и централизованным управлением, такие сети характеризуются высокой степенью адаптивности, гибкости и отсутствием формализованной структуры. Участники этих сетевых образований

[9] Mark in the metaverse. Facebook's <*> CEO on why the social network is becoming "a metaverse company". 22.07.2021. URL: https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview. (Принадлежит компании Meta, которая признана экстремистской организацией и запрещена в России); Kim J. Advertising in the Metaverse: Research agenda // Journal of Interactive Advertising. 2021. Vol. 21. No. 3. P. 141 - 144.

[10] Ball M. Framework for the Metaverse. 29.01.2021. URL: https://www.matthewball.vc/all/forwardtothemetaverseprimer.

специализируются на выполнении узкопрофильных задач в рамках общей криминальной деятельности, что способствует формированию специфического сегмента криминального рынка, известного как "Преступление как услуга".

В рамках данной модели предоставляются услуги по разработке вредоносного программного обеспечения, несанкционированному доступу к информационным системам, созданию фишинговых ресурсов, легализации криптовалют и организации распределенных атак отказа в обслуживании (DDoS-атаки). Данная форма организации преступной деятельности представляет собой качественно новый уровень криминального предпринимательства, где криминальные услуги становятся товаром, доступным для широкого круга пользователей на условиях аутсорсинга.

Вопросы юрисдикции и правоприменения в контексте деликтных правонарушений, совершенных в метавселенных, представляют собой одну из наиболее актуальных и многогранных проблем в области криминологии и международного права. Глобализация метавселенных, неопределенность в идентификации места совершения противоправных деяний и сложности в установлении личности правонарушителей создают значительные вызовы для эффективного противодействия киберпреступности в цифровом пространстве [8]. Развитие метавселенных требует системного подхода к определению юрисдикции, разработки специализированных механизмов международного сотрудничества и адаптации традиционных правовых институтов к реалиям цифровой экосистемы. Особое внимание следует уделить криминализации новых форм противоправного поведения в метавселенных, не имеющих прямых аналогов в физическом мире, таких как виртуальное насилие, кража цифровой идентичности и незаконное присвоение виртуальных активов.

Количество киберпреступлений растет и будет расти в связи с тем, что результативность самого преступления не связана с большим риском для виновного лица, особенно это касается условий виртуальной среды. В реальном мире психологический аспект совершения преступления предполагает наличие некоторых средств сдерживания, внешних и внутренних обстоятельств, без преодоления которых невозможно достижение преступной цели. В условиях метавселенной, преступник, использующий цифровой аватар, не видит свою жертву. Он также общается с цифровым аватаром, принадлежность которого не всегда может быть установлена на момент совершения преступления. Также необходимо учитывать, что в качестве посягательства может быть выбран не отдельный человек, а организация, их множество, целое государство.

Список литературы

1. Лескина Э.И. Метавселенная и задачи в области правового регулирования данных // Юрист. 2023. N 3. С. 22-25.

2. Овчинников А.И., Ширинских П.И. Метавселенные и право: вызовы новых технологий в условиях дальнейшего развития Интернета // Вестник юридического факультета Южного федерального университета. 2023. Т. 10. N 2. С. 18-26.

3. Хабриева Т.Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. N 9. С. 15.

4. Ball M. Framework for the Metaverse. 29.01.2021. URL: https://www.matthewball.vc/all/forwardtothemetaverseprimer.

5. Mark in the metaverse. Facebook's <*> CEO on why the social network is becoming "a metaverse company". 22.07.2021. URL: https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview. (Принадлежит компании Meta, которая признана экстремистской организацией и запрещена в России); Kim J. Advertising in the Metaverse: Research agenda // Journal of Interactive Advertising. 2021. Vol. 21. No. 3. P. 141 - 144.

6. Johnson D.R., Post D.G. Law and Borders - The Rise of Law in Cyberspace // Stanford Law Review. 1996. Vol. 48. P. 1367 - 1402.

7. Wang Y., Su Z., Zhang N. [et al.]. A Survey on Metaverse: Fundamentals, Security, and Privacy // arXiv:2203.02662v4.

8. Бегишев, И. Р. Об обороте роботов, их составных частей (модулей) (инициативный проект федерального закона) : Препринт № 1 за 2021 г. / И. Р. Бегишев ; Казанский инновационный университет им. В. Г. Тимирясова; Бегишев И. Р.. – Казань : Издательство "Познание", 2021. – 28 с. – ISBN 978-5-8399-0662-4. – EDN FTFKAN.

УДК 343.98

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

Использование технологий искусственного интеллекта в расследовании преступлений: российский и зарубежный опыт

Аннотация. Основной целью исследования настоящей статьи является рассмотрение современных возможностей применения технологии искусственного интеллекта в расследовании преступлений. Указываются современные сферы применения искусственного интеллекта. Особое внимание уделено зарубежному опыту внедрения технологий искусственного интеллекта в расследование преступлений. Приводятся технологии, на базе искусственного интеллекта которые, уже успешно применяются в зарубежных странах, опыт которых можно учитывать и при внедрении у нас в стране.

Ключевые слова: цифровизация, технологии, искусственный интеллект, сферы применения нейросетей, BigData, расследование преступлений, российский и зарубежный опыт

V. A. Dudarev,
Senior Lecturer,
Bryansk State University
named after Academician I.G. Petrovsky

Using artificial intelligence technologies in crime investigation: Russian and foreign experience

Abstract. The main objective of the present article is to consider modern possibilities of using artificial intelligence technology in crime investigation. Modern areas of artificial intelligence application are indicated. Particular attention is paid to foreign experience in implementing artificial intelligence technologies in crime investigation. Technologies based on artificial intelligence are given, which are already successfully used in foreign countries, the experience of which can be taken into account when implementing in our country

Keywords: digitalization, technologies, artificial intelligence, areas of application of neural networks, BigData, crime investigation, Russian and foreign experience.

Введение. В середине XX века в 1956 г. появились алгоритмы, которые позволяли моделировать процесс мышления человека, благодаря чему и появился термин искусственный интеллект (Artificial Intelligence, AI).Однако только лишь в XXI веке благодаря накоплению большого объема данных (BigData), эти алгоритмы были

усовершенствованы, что позволило оптимизировать вычислительные мощности, и искусственный интеллект стал очень актуальной и популярной технологией.

XXI век – век современных технологий, инноваций и развития. В последние годы в нашей стране активное развитие получает цифровизация практически во все сфер нашего общества, катализатором которой отчасти послужила пандемия COVID-19. Сферы уголовного судопроизводства и криминалистики также не являются исключением [3, 4]. Одной из таких технологий, которая в последнее время быстро и хорошо себя зарекомендовала практически во всех сферах нашей жизни – является искусственный интеллект (далее – ИИ).

Основная часть. ИИ является инновационным инструментом, оказывающим влияние на всю цифровизацию нашей страны охватываемую сферами экономики, науки, образования, медицины и т.д. Сейчас благодаря ИИ охвачено большое количество сфер жизнедеятельности человека, будь то игра в шахматы, генерация изображений, доказательство математических теорем, диагностика заболеваний или расследование преступлений.

Однако повсеместное использование цифровых технологий способствует и совершенствованию тех или иных преступлений, на что правоохранители не могут не обращать внимания. Как сообщил заместитель начальника следственного департамента МВД РФ Данил Филиппов, ущерб от IT-преступлений за первые пять месяцев 2025 года составил 81 миллиард рублей, что почти на четверть больше, чем за аналогичный период прошлого года [1].

Технологии ИИ уже активно внедряются в сферу работы правоохранительных органов.

Основными возможностями использования ИИ в расследовании преступлений являются:

– способность современных компьютеров гораздо быстрее обрабатывать большие объемы информации (BigData) для анализа криминалистически значимой информации;

– географическое профилирование (метод уголовного расследования, который анализирует места совершения взаимосвязанных преступлений для определения наиболее вероятного района проживания преступника);

– исследование деятельности экстремистских групп во избежание осуществления информационного теракта [8.С. 114];

– быстрый анализ метаданныхи иной цифровой информация, содержащейся на различных устройствах [9. С. 201].

На сегодняшний день уже разработано большое количество нейросетей в самых различных сферах применения:

1) нейросети для создания сайтов: Craftum AI[11]; Framer[12]; Designs AI; Unbounce[13]; 10Web[14];

2) нейросети для генерации текста:ChatGPT[15], Gemini[16], YandexGPT[17]; CopyMonkey, HypotenuseAl, Copy.ai;

3) нейросети для генерации изображений (Midjourney[18], StableDiffusion[19], Craiyon, Шедеврум[20], Kandinsky 3.0[21];

4) нейросети для озвучки (SteosVoice[22], Zvukogram, Voicemaker[23], PodcastleAi, Genny;

5) нейросети для создания видео: Visper[24], Fliki[25], Veed.io, Synthesia, Lumen5[26].

Если обратиться к зарубежному опыту применения технологий искусственного, то в нем можно найти немало примеров успешного внедрения этой технологии в правоохранительную деятельность.

В США Федеральное Бюро Расследований (ФБР) использует ИИ для распознавания правонарушителей на видео с камер наблюдения в режиме реального времени [13]. В США также существует программа распознавания граждан по фрагментам татуировок [11].

---

[11] Российский инновационный сервис, способный сгенерировать сайт за 3 минуты с помощью нейросети.

[12] Конструктор с генерацией сайта нейросетью, поддерживает одностраничники, блоги, корпоративные проекты.

[13] Конструктор с возможностями нейросети, ориентированный преимущественно на целевые страницы

[14] Инструмент для создания сайтов на основе искусственного интеллекта, который облегчает процесс разработки, не требуя от пользователей глубоких технических знаний.

[15] Одна из самых крупных и популярных, наделена широким функционалом, но чаще всего используется именно для генерации текстов.

[16] Передовая нейросеть, предназначенная для генерации текста, которая включает в себя несколько уровней.

[17] Передовой инструмент от Яндекса, его можно открыть и бесплатно использовать прямо из браузера (через иконку Алисы).

[18] Нейросеть в вопросе рисования и генерации изображений, предлагающая массу параметров для настройки.

[19] Сервис позволяет создавать фотореалистичные изображения, используя модель глубокого обучения, способную анализировать и улучшать качество картинок.

[20] Проект Яндекса, доступный только в одноименном мобильном приложении. Легко создает картинки и анимацию по запросам, а также генерирует видео на основе изображений.

[21] Третья версия AI инструмента от «Сбера», доступна на сайте и в ботах Телеграм, ВКонтакте. Позволяет создавать фотореалистичные изображения по текстовым запросам, легко управлять стилями и прочими параметрами.

[22] Располагает AI инструментами для создания уникального контента и подкастов, озвучивания любых видео, монетизации собственного голоса.

[23] Инструмент для преобразования текста в речь, поддерживает свыше 1000+ образцов AI голосов и популярные языки, в том числе и русский.

[24] Нейросеть для быстрого создания видео, осуществляет преобразование текста в эффектный контент.

[25] Быстрый видеогенератор с искусственным интеллектом, способный оживить любые идеи.

[26] Современный мощный инструмент для генерирования видеороликов из текста.

Применяемое Департаментом полиции Чикаго прогностическое программное обеспечение характеризуется способностью с высокой степенью вероятности определять как круг лиц, потенциально способных совершить преступление, так и круг лиц с повышенной виктимологической уязвимостью. Об эффективности системы свидетельствует то, что более 70% человек из списка потенциальных жертв были убиты в течение года [5. С. 27].

Пьяный житель Лос-Анджелеса попытался угнать беспилотный электромобиль Jaguar I-PACE сервиса вызова роботакси. Но авто было хитрее: оно заблокировало двери и сообщило об инциденте в полицию. В компании-производителе заявили, что их автомобили спроектированы таким образом, чтобы предотвратить управление ими посторонними лицами. По словам представителей компании, за более чем 5 млн. выполненных поездок было всего несколько попыток несанкционированного управления их автомобилями [12].

Ведутся разработки, позволяющие читать по губам (LipNet, распознает текст с точностью до 93%) и по колебаниям кожи лица; считывать мысли человека, воспроизводить то, что человек видел и читал ранее, его фантазии [5]. Все это может использоваться правоохранительными органами для раскрытия и расследования преступлений.

Великобритания стала первой страной в мире, которая ввела новые уголовные статьи, касающиеся сексуального насилия с использованием ИИ, для защиты детей от онлайн-преступников. В рамках новых законопроектов, вводятся уголовные статьи, которые делают незаконным владение, создание и распространение инструментов ИИ, предназначенных для генерации детской порнографии. Также после получения доступа к устройству будет использована специальная технология для сравнения содержимого устройства с базой данных изображений, содержащих сцены насилия над детьми (CAID) [2].

В Великобритании следствие будут вести роботы-знатоки. ИИ менее чем за 2 дня может оценить доказательства, на которые человеку потребовался бы 81 год. Начальники полиции надеются, что технология может помочь детективам определить новые направления нераскрытых дел [6].

В Таиланде представили первого полицейского робота с ИИ. Робот оснащен круговой камерой и подключен к системе видеонаблюдения. Аппарат в режиме реального времени получает данные от дронов, анализирует происходящее на улицах и отправляет собранную информацию в центр управления. Одна из главных функций робота-полицейского – распознавание лиц, он может определить, находится ли человек в розыске или входит в группу риска [7].

Китайские ученые представили модель, способную воссоздавать 3D-изображения лица человека на основе его генетических данных. Разработанная технология получила название Diffface, она анализирует различия в отдельных нуклеотидах ДНК и сопоставляет их с так называемыми облаками точек – цифровыми

3D-моделями поверхности лица. Технология была протестирована на базе данных с участием представителей народности хань: использовались более 9 тыс. пар генетических и 3D-изображений. Технология Difface может не только воссоздавать трехмерное изображение лица человека по его ДНК, но и прогнозировать, как оно будет выглядеть в будущем [10]. Разработка может найти применение в криминалистике, в том числе при расследовании преступлений по генетическим следам, оставленным на месте происшествия.

Заключение. Таким образом, на сегодняшний день и в России, и в зарубежных странах при расследовании преступлений активно используются технологии, связанные с ИИ. Его применение в криминалистике способно решать такие задачи: 1) выявлять различные следственные ошибки; 2) сокращать время расследования преступлений благодаря быстрому анализу большого объема баз данных; 3) способность к прогнозированию будущих преступлений.

В нашей стране необходимо продолжать разработки технологий ИИ с опорой на опыт зарубежных стран необходимый для борьбы с преступностью, а также внедрение таких технологий в криминалистику для быстрого и качественного раскрытия и расследования различных видов преступлений.

Список литературы

1. В МВД оценили ущерб от IT-преступлений // https://ria.ru/20250618/it-prestupleniya-2023640268.html (дата обращения: 01.08.2025).

2. Великобритания стала первой страной в мире, которая ввела новые уголовные статьи, касающиеся сексуального насилия с использованием искусственного интеллекта // https://wikivisa.ru/blog/britanskie-advokaty/ (дата обращения: 01.08.2025).

3. Дударев В. А. Пандемия COVID-19 как катализатор цифровизации российского уголовного судопроизводства // Уголовная юстиция. 2021. № 17. С. 39–43.

4. Дударев В. А. Цифровизация уголовного судопроизводства России: плюсы и минусы // Научное обозрение. Серия 1: Экономика и право. 2021. № 2. С. 151–161.

5. Жданов Ю. Полиция будущего / Ю. Жданов, В. Овчинский. М., 2018. 166 с.

6. Искусственный интеллект может быть использован для раскрытия самых громких дел // https://vk.com/wall-70187376_6564941 (дата обращения: 01.08.2025).

7. Киборг 1.0: тайский Робокоп патрулирует улицы с помощью 360° глаз и возможности отслеживания лиц в реальном времени // https://interestingengineering.com/innovation/ai-thai-robocop-patrols-stree (дата обращения: 01.08.2025).

8. Коломинов В. В. Особенности расследования преступлений с использованием искусственного интеллекта // Юристъ-Правоведъ. 2023. № 4(107). С. 112 – 117.

9. Маевский С. С., Дударев В. А. Особенности раскрытия и расследования преступлений, совершаемых в сфере незаконного оборота наркотических средств, с использованием правоохранительными органами новых направлений криминалистики // Эпомен. 2021. № 59. С. 193 – 206.

10. Новая ИИ-модель может создать 3D-портрет человека по его ДНК // https://trends.rbc.ru/trends/innovation/ (дата обращения: 01.08.2025).

11. Обзор отдельных вопросов в области больших данных и искусственного интеллекта / под ред. В.С. Овчинского. М.: ГИАЦ МВД России, 2019. С. 53 – 54.

12. Роботакси задержало автоугонщика и сдало его полиции // https://dzen.ru/a/Z3qTPCbj0llJRX5u (дата обращения: 01.08.2025).

13. Яцуценко В. В. Проблемы и перспективы внедрения цифровых технологий в деятельность органов прокуратуры / В. В. Яруценко. // Актуальные проблемы российского права. 2021. № 11. С. 187 – 192.

УДК 343.9.01

И. И. Евтушенко,
кандидат юридических наук, доцент,
Крымский филиал Краснодарского университета МВД России

О возможности самозащиты от мошенничеств покупателей недвижимости в условиях ограниченности использования персональных данных других лиц

Аннотация. Статья посвящена анализу правовой коллизии между необходимостью самозащиты покупателей недвижимости от мошенничества и ограничениями, налагаемыми законодательством о защите персональных данных. Рассматривается невозможность добросовестного покупателя легально проверить благонадежность продавца на этапе принятия решения о сделке. Отмечается, что отмена публичного доступа к полным сведениям ЕГРН и запрет на сбор персональных данных без согласия субъекта, лишают покупателя эффективных инструментов превентивной проверки. Подчеркивается, что получение согласия продавца на доступ к его персональным данным требует внесения задатка, который может быть утрачен при отказе от рискованной сделки. Констатируется подход судов, возлагающий ответственность за действительность сделки на покупателя при отсутствии четкого стандарта добросовестности. Делается вывод о системной виктимизации покупателей вследствие правового пробела, требующего сбалансированных механизмов верификации контрагента.

Ключевые слова: самозащита прав покупателя, мошенничество с недвижимостью, персональные данные, виктимизация покупателя недвижимости, проверка продавца, правовой пробел

I. I. Evtushenko,
Master of Law, Associate Professor,
Crimean Branch of Krasnodar University of the Interior Ministry of Russia

About the possibility of self-defense against fraud by realty buyers in conditions of limited use of other persons' personal data

Abstract. This article examines the legal conflict between the need for self-protection of real estate buyers against fraud and the restrictions imposed by personal data protection legislation. It highlights the impossibility for bona fide buyers to legally verify a seller’s reliability during pre-transaction due diligence. The analysis emphasizes that the revocation of public access to complete Unified State Register of Real Estate (USRN/EGRN) data and the prohibition on collecting personal data without consent deprive buyers of effective preventive verification tools. The study notes that obtaining seller consent often requires substantial advance payments (deposits), which are forfeited if the buyer withdraws from a

high-risk transaction. Judicial practice shifting responsibility to buyers amid the absence of clear good-faith standards is critically assessed. The article concludes that systemic victimization of buyers stems from a regulatory gap requiring balanced counterparty verification mechanisms.

Keywords: buyer's rights self-protection, real estate fraud, personal data, victimization buyer of realty, seller due diligence, regulatory gap

Введение. Захлестнувшая Россию волна дистанционных мошенничеств в финансово-кредитной сфере деятельности сместила фокус внимания государственных, в том числе правоохранительных органов, с куда более тяжких проявлений преступной деятельности – мошенничеств с жилыми помещениями, в результате которых люди утрачивают даже единственное жилье как бы по собственной воле, будучи введенными в заблуждение легендой мошенников об участии в специальной операции правоохранительных органов по поиску мошенников или террористов.

Основная часть. Хотелось бы обратить внимание на такую значимую для каждого владельца недвижимости проблему как возможность превентивной самозащиты своего права при приобретении квартиры на вторичном рынке, да и в новостройках тоже. Напрямую в Уголовном кодексе Российской Федерации (далее - УК РФ) не закреплено право граждан на превентивную самозащиту от преступлений, оно лишь презюмируется через трактовку положений главы 8 «Обстоятельства, исключающие преступность деяния» и установление критериев превышения мер (то есть признаков уголовно наказуемой самозащиты) при необходимой обороне, задержании преступника, крайней необходимости. Аналогичным образом самозащита допускается и статьями 448 и 449 Гражданского кодекса Российской Федерации (далее – ГК РФ).

Профессор В.П. Грибанов предлагает под самозащитой понимать «совершение управомоченным лицом дозволенных законом действий фактического порядка, направленных на охрану его личных или имущественных прав и интересов. Необходимо различать предпринимаемые управомоченным лицом для самозащиты своих прав меры превентивного характера и меры активно-оборонительного характера» [2].

В учебнике по гражданскому праву авторы выделяют юрисдикционную и неюрисдикционную формы защиты в качестве основных [1. С. 254-256].

В этом контексте мы рассмотрим неюрисдикционную превентивную виктимологическая защиту «полностью невиновного» (по классификации Б. Мендельсона) покупателя недвижимости (квартиры, жилого дома, земельного участка). Может ли он, пользуясь имеющимися у него весьма ограниченными возможностями как непрофессионального участника рынка недвижимости, распознать мошеннический обман в отношении него? Может ли он использовать свое право на

превентивную самозащиту? Могут ли профессиональные участники рынка недвижимости распознать мошенника, которым по сути в сделке выступает «ведомый» продавец, тщательно скрывающий свой обман и от риелтора, и от покупателя недвижимости, по сути сознательно обманывающий покупателя (так называемая «жертва-преступник»)?

Согласно ГК РФ все сделки делятся на две большие группы:

– ничтожные (то есть абсолютно недействительные по своей сути с момента их заключения – с пороком формы, с пороком содержания и совершенные лицами, которые их не могут совершать ни и каких условиях) и

– оспоримые (то есть относительно недействительные с момента признания их таковыми судом – с пороком воли субъектов и совершенные лицами, не обладающими полной дееспособностью).

То есть, проверку будущей недвижимости необходимо разделить на две составляющие: проверка самого объекта недвижимости и проверка продавца.

Проверка объекта недвижимости направлена на выявление пороков ее легитимности начиная с момента приобретения права у исходного правообладателя. То есть будущий покупатель, чтобы быть уверенным что и его сделку в будущем никто не оспорит, должен быть уверен в легитимности всей цепочки сделок с этим объектом недвижимости. В разные исторические периоды юридическое оформление прав правообладателей существенно отличалось (например, в сельской местности велись похозяйственнее книги, также фиксацию прав на объекты недвижимости осуществляли органы БТИ, а с 1998 года – Росреестр). И что бы привести все ранее приобретенные права на недвижимость к единому знаменателю, при совершении сделок возможна одновременная и регистрация права собственности за первоначальным владельцем, и переход права от него к новому правообладателю. То есть, на сегодняшний день государство через систему государственной регистрации прав на недвижимое имущество и сделок с ним гарантирует стабильность оборота недвижимости, защищает интересы всех участников рынка недвижимости и третьих лиц, с которыми у собственников недвижимости могут возникнуть обязательства. Как устанавливает ч. 2 ст. 1 Федерального закона «О государственной регистрации недвижимости» «Единый государственный реестр недвижимости является сводом достоверных систематизированных сведений об учтенном в соответствии с настоящим Федеральным законом недвижимом имуществе, о зарегистрированных правах на такое недвижимое имущество, основаниях их возникновения, правообладателях, а также иных установленных в соответствии с настоящим Федеральным законом сведений» [3].

Именно поэтому проверка объекта недвижимости начинается с запроса информации из Росреестра. До недавнего времени сведения о любом объекте недвижимости и его правообладателях, а также о всех сделках, совершенных с данным объектом, мог за плату запросить любой желающий на официальном сайте Росреестра (https://rosreestr.gov.ru/). В выписке из Единого государственного реестра

недвижимости (далее – ЕГРН) указывались: основные юридически значимые сведения об объекте недвижимости, вид зарегистрированного права на него, сведения об ограничениях прав и обременениях объекта недвижимости, правообладателях с указанием их паспортных данных, документах-основаниях государственной регистрации прав. Однако изменениями, внесенными в федеральный закон, с 01.03.2023 принцип открытости сведений о недвижимости был изменен, получить полные сведения из Росреестра может только сам правообладатель (даже в случае оформления квартиры в ипотеку при проведении проверок кредитной организацией), или нотариус при наличии определенных условий. А значит получить полную, объективную и достоверную информацию будущий покупатель не может: только если такой доступ ему даст продавец. Сделано это было в целях защиты персональных данных правообладателей от неправомерного их собирания и использования третьими лицами. Кроме того, оборот недвижимости значительно упрощен, сделки совершаются дистанционно с помощью электронных цифровых подписей, право собственности подтверждается только выпиской из ЕГРН.

Однако права будущего покупателя в данном случае страдают: на первоначальном этапе, при принятии решения о приобретении или нет объекта недвижимости он вынужден верить только информации, представленной продавцом в виде электронной выписки из ЕГРН. На сегодняшний день приобретение недвижимости на вторичном рынке представляет собой уравнение со многими неизвестными – даже при полной проверке всех возможных рисков не стать жертвой мошенничества крайне сложно.

Может ли будущий покупатель иным образом проверить легитимность самого объекта и прав на него?

Может, но весьма в ограниченном объеме, буквально по крупинкам собирая косвенную информацию из открытых источников – легально существующих открытых баз данных. Например, официальном сайте застройщика или с помощью различных сервисов ФНС России. Физическое лицо также можно проверить по различным официальным онлайн сервисам, если продавец согласился предоставить свои персональные данные. Такая проверка помогает исключить риски в будущем признания заключенной сделки недействительной и обращения взыскания на имущество продавца по различным основаниям: по закону об исполнительном производстве, о банкротстве, о противодействии терроризму и экстремизму, государственной службе и т.д.

Может ли будущий покупатель собирать иную – неофициальную, но открытую информацию о продавце и его недвижимости? Например, получить сведения об упоминании о нем из интернета, социальных сетей, проанализировать историю продаж на онлайн площадках объявлений? Или выяснить историю самой квартиры, в какой обстановке ему предстоит жить, поговорить с соседями, родственниками продавца, есть ли неприязненные отношения с кем-либо из соседей, споры за общие

пространства, парковки, коммунальные долги, неправомерные действия, нарушения общественного порядка и т.п.?

Следует отметить, что персональные данные о лице, которые он сам разместил в открытых источниках, хоть и являются общедоступными, но не являются свободно обращаемыми. В своем исследовании З. Го отмечает, что «хотя незаконное использование обычной личной информации менее опасно, чем незаконное использование конфиденциальной личной информации, преступники, которые явно не уважают личную информацию обычных граждан, с большей вероятностью будут навязывать ее обычным гражданам» [6].

Как отмечает Е.В. Хохлова, «в теории уголовного права научные споры вызывают подходы к установлению вины в отношении сбора или распространения общедоступных персональных данных, квалифицируемых, как правило, по ст. 137 «Нарушение неприкосновенности частной жизни» Уголовного кодекса Российской Федерации. Дискуссия касается неопределенности в понимании того, когда тайна персональных данных может быть нарушена правомерно» [4. С. 214]

Ответ на этот вопрос дал Пленум Верховного Суда РФ в п. 2 Постановления № 46 от 25 декабря 2018 г. отметив, что «не может повлечь уголовную ответственность собирание или распространение таких сведений в государственных, общественных или иных публичных интересах, а также в случаях, если сведения о частной жизни гражданина ранее стали общедоступными либо были преданы огласке самим гражданином или по его воле». В п. 3 устанавливается, что «под собиранием сведений о частной жизни лица понимаются умышленные действия, состоящие в получении этих сведений любым способом, например, путем личного наблюдения, прослушивания, опроса других лиц, в том числе с фиксированием информации аудио-, видео-, фотосредствами, копирования документированных сведений, а также путем похищения или иного их приобретения».

То есть тот факт, что соседи могут непроизвольно наблюдать жизнь других соседей, не дает им права эту информацию собирать, распространять, передавать третьим лицам. Вся эта информация может быть получена двумя законными способами: с согласия правообладателя или на основании судебного решения в рамках оперативно-розыскных мероприятий по возбужденному уголовному делу. Получается, что в соответствии с федеральным законом «О защите персональных данных» без письменного согласия субъекта персональных данных их собирать и использовать покупателю запрещено, а самовольный сбор неформальной информации о продавце может повлечь уголовную ответственность по ст. 137 или даже 272^1 УК РФ.

Однако и со стороны продавца дача согласия на сбор, обработку и использование его персональных данных каждому позвонившему по объявлению лицу, которым также может быть мошенник – не является разумной. Случаи подделки доверенностей по полученным от собственника персональным данным и последующей мошеннической

перепродажей недвижимости также до сих пор встречаются в судебно-следственной практике.

Возможно ли покупателю отказаться от проведения подобных проверок, всецело полагаясь на заверения продавца о его добросовестности?

Как показывает анализ судебной практики рассмотрения дел о признании сделок недействительными, суды всю ответственность за сделку при покупке недвижимости перекладывают на покупателя, требуя от него доказательств его добросовестности, незнания о пороках самой сделки, ее объекта и воли продавца. И тогда покупатель вынужден доказывать, что он предварительно проверил объект продажи всеми доступными ему способами, проверил дееспособность самого продавца, при чем он должен хранить все доказательства собственной добросовестности на случай оспаривания сделки в суде. Более того, признание оспоримой сделки недействительной или применение последствий ничтожности сделки в виде двусторонней реституции не позволяет покупателю компенсировать понесенные расходы на оказание ему юридических услуг, оплату государственной пошлины при подаче встречного иска, так как он оказывается проигравшей стороной.

При этом позиции судов таковы, что далеко не всегда покупатель может быть признан добросовестным. В п. 1 Постановления Пленума Верховного Суда РФ от 23.06.2015 № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации» указано то, что «Оценивая действия сторон как добросовестные или недобросовестные, следует исходить из поведения, ожидаемого от любого участника гражданского оборота, учитывающего права и законные интересы другой стороны, содействующего ей, в том числе в получении необходимой информации». При этом стандарт добросовестного поведения в сделках с недвижимостью четко не сформулирован. Суд устанавливает его исходя из конкретных обстоятельств дела.

В итоге, законодатель, пытаясь защитить интересы субъекта персональных данных, делает крайне затруднительной процедуру самостоятельной проверки объекта недвижимости и личность продавца до принятия решения о заключении сделки. Как правило, стороны сначала заключают предварительный договор или соглашение о задатке, после чего продавец дает согласие на обработку информации о нем. Однако суммы задатка достигают весьма существенных размеров. И в случае выявления рисков для покупателя и его последующего отказа от заключения рискованной сделки, этот задаток остается у продавца, который скрыл юридически значимую информацию от покупателя. То есть покупатель оказывается в ловушке: чтобы получить доступ к информации и получить согласие продавца на проверку, покупатель вынужден внести крупный задаток под угрозой его потери. При этом покупатель безоружен: нет эффективных легальных инструментов для превентивной проверки продавца на этапе принятия решения.

Таким образом, существующее правовое регулирование способствует виктимизации населения через систему ограничения доступа к персональным данным владельцев недвижимости и сведениям об объектах недвижимости, полагая что только обращение к нотариусу способно учесть интересы обеих сторон. Однако принятие решения о заключении сделки у нотариуса принимается уже после достижения сторонами соглашения о задатке или подписании предварительного договора купли-продажи – добросовестный покупатель несет финансовые потери или вынужден идти на риск.

Вместе с тем, ситуация не является тупиковой. Например, можно разрешать доступ к данным покупателю через авторизацию на Госуслугах с уведомлением продавца о запросе этих данных и получении от него согласия (или отказа) до момента передачи задатка, но после ознакомления с первоначальной документацией, предоставленной продавцом. Это значительно снизит риски продавца стать жертвой мошенничества, поскольку он будет оповещен о запросе конкретного авторизованного пользователя, а последний не сможет остаться анонимным (что и сделало дистанционные мошенничества очень популярными).

На западе используется и такой способ самозащиты прав пользователей как уведомление о компрометации его персональных данных [5]. Полагаем, что такой способ нельзя признать эффективным именно как способ самозащиты, поскольку потерпевшей стороне остается только минимизировать потери от действий злоумышленников. Такая политика приводит к конфликту интересов жертв при использовании мошенниками все новых цифровых криминальных методик. К сожалению, «ответственность за самозащиту от кражи личных данных, возложенная на отдельных потребителей, подразумевает, что граждане не должны рассчитывать на поддержку государства, несмотря на то что правительства и частные компании регулярно используют уязвимые информационные системы» [7].

Заключение. На сегодняшний день мы видим, что на уровне правового регулирования баланс интересов продавца и покупателя на стадии предварительной проверки объекта недвижимости отсутствует. Покупатель только тогда сможет провести проверку объекта недвижимости, когда продавец предоставит ему критически важные персональные сведения, что становится уже небезопасным для самого продавца, повышает его виктимность и риск стать жертвой мошенников. Становится очевидным, что и покупателю, не являющемуся профессиональным юристом, и даже являющимся таковым, затруднительно реализовать свое право на превентивную самозащиту в виду закрытости информации о продавце и объекте недвижимости.

Список литературы

1. Гражданское право. Учебник. В 3 т. Т. 1 / Под ред. А.П. Сергеева, Ю.К. Толстого. М. 2018.

2. Грибанов В.П. осуществление и защита гражданских прав // URL: https://civil.consultant.ru/elib/books/1/page_13.html (дата обращения: 16.07.2025).

3. Федеральный закон от 13.07.2015 № 218-ФЗ (ред. от 26.12.2024) «О государственной регистрации недвижимости» // https://www.consultant.ru/document/cons_doc_LAW_182661/ (дата обращения: 24.02.2025).

4. Хохлова Е. В. Персональные данные в социальных сетях: теория и судебная практика толкования общедоступности // Научный вестник Омской академии МВД России. 2023. Т. 29, № 3(90). С. 214–219.

5. Gibson D., & Harfield C. Amplifying victim vulnerability: Unanticipated harm and consequence in data breach notification policy. International Review of Victimology, 29(3), (2022). P. 341-365. // URL: https://doi.org/10.1177/02697580221107683/ (дата обращения: 24.02.2025).

6. Guo Z. Criminalisation of the illegal use of personal data: comparative approaches and the Chinese choice. Humanit Soc Sci Commun 12, (2025). P. 782. // URL: https://doi.org/10.1057/s41599-025-05141-y (дата обращения: 24.02.2025).

7. Reynolds D. Everyone is victimized or only the naïve? The conflicting discourses surrounding identity theft victimization. International Review of Victimology, *29*(3), (2022). P. 449-465. // URL: https://doi.org/10.1177/02697580221091284 (дата обращения: 24.02.2025).

УДК 343.34

Р. Э. Гильманов,
аспирант
Казанский инновационный университет
имени В.Г. Тимирясова,
В. В. Еремкин,
магистрант,
Казанский инновационный университет
имени В.Г. Тимирясова

Уголовно-правовая характеристика объекта и объективной стороны неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Аннотация. Критическая информационная инфраструктура (далее – КИИ) давно стала нервной системой экономики и государственного управления, и в моменты технологических и геополитических турбуленций она неизбежно превращается в мишень для злоумышленников. По данным исследования «InfoWatch», опиравшегося на статистику МВД и материалы ГАС Правосудие, в 2021 году Россия столкнулась с резким всплеском уголовных дел, связанных с кибератаками и иным неправомерным воздействием на объекты КИИ. Если в 2020 году было 22 таких дела, то уже в 2021-м их стало 70, то есть увеличилось более чем в три раза. Динамика правоприменения в 2022 г. указывает на ускорение процесса криминализации противоправных действий против КИИ. Исходя из данных МВД России, за указанный период зарегистрировано 519 преступлений по ст. 274.1 УК РФ, что означает рост на 226,41 % по сравнению с предыдущим отчетным периодом. Это подчеркивает необходимость и актуальность анализа особенностей объекта и объективной стороны неправомерного воздействия на критическую информационную инфраструктуру.

Ключевые слова: критическая информационная инфраструктура; неправомерное воздействие на критическую информационную инфраструктуру; объективная сторона преступления; информационная безопасность

R.E.Gilmanov,
Postgraduate student
Kazan Innovative University named after V. G. Timiryasov**,**
V.V. Eremkin,
Master's student
Kazan Innovative University named after V. G. Timiryasov

Criminal and legal characteristics of the object and the objective side of the unlawful impact on the critical information infrastructure of the Russian Federation

Annotation. Critical information infrastructure has long been the nervous system of the economy and public administration, and in times of technological and geopolitical turbulence, it inevitably becomes a target for intruders. According to an InfoWatch study based on statistics from the Ministry of Internal Affairs and materials from GAS «Pravosudie» («Justice»), in 2021 Russia faced a sharp surge in criminal cases related to cyber attacks and other unlawful effects on CII facilities. If 22 such cases were recorded in 2020, then in 2021 there were 70 of them, that is, the growth exceeded the three-fold threshold.

The law enforcement dynamics of 2022 records the acceleration of the process of criminalization of illegal actions against the CII. According to the Russian Interior Ministry, 519 crimes were registered during this period under Article 274.1 of the Criminal Code of the Russian Federation, which means an increase of 226.41% compared to the previous reporting period. This underlines the need and relevance of analyzing the features of the object and the objective side of the unlawful impact on the critical information infrastructure.

Keywords: critical information infrastructure; unlawful impact on critical information infrastructure; objective side of crime; information security

Введение. Уголовно-правовая характеристика объекта и объективной стороны неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации закрепляет ответственность за посягательства на критическую информационную инфраструктуру Российской Федерации как на особый охраняемый объект. Под видовым объектом составов, объединенных в статье, должна пониматься безопасность критической информационной инфраструктуры, понимаемая как состояние защищенности от любого программного или программно-технического воздействия, способного вызвать нарушение функционирования соответствующих систем или поставить под угрозу безопасность обрабатываемой ими информации.

Правоприменительная динамика 2022 года подчеркивает ускорение процесса криминализации противоправных действий против КИИ. По данным МВД России, за этот период зарегистрировано 519 преступлений по ст. 274.1 УК РФ, что означает рост на 226,41 % по сравнению с предыдущим отчетным периодом. Одновременно важно отметить, что по информации Судебного департамента при Верховном Суде РФ, в том же 2022 году судом было осуждено 57 человек. Если сопоставить эти цифры, станет заметным снижение доли дел, доведенных до приговора, в сравнении с количеством зарегистрированных преступлений, что можно объяснить факторами процедурного и доказательственного характера.

Основная часть. Непосредственный объект посягательства конкретизирует эту защиту и объединяет охраняемую компьютерную информацию и средства ее защиты в совокупности с телекоммуникационными системами, сетями и иными устройствами,

относящимися к критической информационной инфраструктуре. Такая конструкция подчеркивает интегральный характер цифровых критических систем, где данные, механизмы их защиты, каналы связи и управляющие компоненты образуют единый технологический контур. Под охраняемой компьютерной информацией понимается информация, на которую установлен правовой режим защиты, и фактически применяются средства ограниченного доступа, а значит, любое незаконное вмешательство в ее обработку или защиту одновременно затрагивает и техническую, и правовую составляющие безопасности [1. С. 30].

Объективная сторона в части первой ст. 274.1 УК РФ охватывает действия, направленные на неправомерное воздействие на критическую информационную инфраструктуру, и включает создание, распространение или использование компьютерных программ либо иной компьютерной информации с целью уничтожения, блокирования, модификации или копирования информации, а также нейтрализации средств ее защиты. Указанный состав относится к формальным и признается оконченным в момент совершения любого из указанных действий, независимо от того, наступили ли фактические последствия в виде нарушения работы систем или утраты защищенности данных. Юридически значимыми признаются целевая ориентированность используемых средств на причинение вреда и их функциональная пригодность для подрыва доступности, целостности или конфиденциальности информации, а также для преодоления защитных механизмов.

Объективная сторона в ч. 2 ст. 274.1 УК РФ включает неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре, в том числе с использованием программ и иной компьютерной информации, предназначенных для неправомерного воздействия на такие объекты или содержащих вредоносные компоненты. Данный состав также формальный и окончен в момент получения незаконного доступа любым из перечисленных или иным противоправным способом. Правовое значение имеет сам факт преодоления установленного режима охраны и вторжения в сферу контролируемого доступа, тогда как извлечение, изменение или уничтожение данных, равно как и наступивший ущерб, не требуются для констатации окончания преступления.

Объективная сторона в ч. 3 ст. 274.1 УК РФ заключена в действиях или бездействии, нарушающих правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре, а также информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления и сетей электросвязи, связанных с ней. В отличие от вышеуказанных двух, данный состав уже материален и признается оконченным при наступлении последствий в виде причинения вреда критической информационной инфраструктуре. Юридически значимыми элементами здесь выступают наличие установленных правил эксплуатации, факт их

нарушения и причинная связь между этим нарушением и вредом, который может выражаться в нарушении функционирования инфраструктурных компонентов, снижении надежности и устойчивости их работы, компрометации информации или иных формах подрыва безопасности.

Взаимосвязь трех частей исследуемого состава преступления выстраивает последовательную систему охраны, в которой пресекаются как подготовительные и инструментальные формы вмешательства, так и сам факт незаконного проникновения в охраняемую среду, а также эксплуатационные нарушения, оборачивающиеся реальным ущербом для инфраструктуры. Первые две части концентрируются на ранних стадиях посягательства и не требуют доказательства наступивших последствий, поскольку уже сама направленность действий на разрушение, блокирование или компрометацию критических систем создает недопустимый риск для общественно значимых функций. Третья часть, напротив, наказывает за нарушение установленного режима эксплуатации, придавая решающее значение наступившему вреду и причинно-следственной связи, что позволяет охватить ситуации, когда угрозы исходят не от внешнего злоумышленника, а изнутри контура эксплуатации через несоблюдение регламентов и стандартов безопасности.

Нужно учитывать, что сами объекты критической инфраструктуры могут быть достаточно разнообразными, что также отражается на содержании их объективной стороны (например, применительно к цифровой безопасности системы здравоохранения [6. С. 55; 3. С. 61]).

В научной дискуссии о предмете охраны статьи 274.1 УК РФ заметны два методологических подхода. К.Н. Евдокимов исходит из индивидуализированного, «правоносительного» понимания объекта преступления, акцентируя охраняемые законом права и интересы собственников компьютерной информации в сфере ее безопасного обращения, а также безопасность функционирования технических устройств, входящих в контур критической информационной инфраструктуры [3. С. 35]. Тем самым объектом посягательства выступают как имущественные и иные права конкретных субъектов на информацию, находящуюся в обороте, так и эксплуатационная надежность материально-технической базы КИИ как совокупности устройств, систем и их защитных средств, обеспечивающих законный режим доступа и обработки данных.

Р.И. Дремлюга, напротив, выводит объект на уровень публично-правовых ценностей и рассматривает его как общественные отношения в сфере цифровой экономики и информационного общества по поводу безопасности критически значимых объектов информационной инфраструктуры. В таком подходе центральным становится не столько титул собственности на сведения или устройства, сколько устойчивость функциональных связей и процедур, поддерживающих жизненно важные цифровые сервисы и процессы, от которых зависят экономика, государственное управление и иные социально значимые сферы [2. С. 24].

Сопоставление этих позиций демонстрирует, что они не противоречат, а дополняют друг друга. Индивидуально-правовой фокус подчеркивает персонализированную сторону охраны - интересы правообладателей информации и владельцев инфраструктурных компонентов. Публично-правовой акцент фиксирует системную значимость КИИ, где нарушение безопасности выходит за рамки частного ущерба и трансформируется в риск для устойчивости цифровой экосистемы в целом. В интегративном прочтении объект преступления по ст. 274.1 УК РФ охватывает и субъективные права участников оборота компьютерной информации, и общественные отношения по обеспечению безопасного функционирования критически важных цифровых систем, что соответствует двойственной природе КИИ как пространства данных и как технологической платформы.

Вопрос о формах проявления объективной стороны неправомерного воздействия на КИИ приобретает практическую остроту в связи с квалификацией бездействия. Ю.В. Трунцевский указывает показательный пример - неустановку обновлений программного обеспечения [4. С. 35]. Если в отношении инфраструктурного узла действуют технические регламенты, корпоративные политики или иные обязательные для исполнителя требования по своевременному обновлению, их игнорирование формирует признак объективной стороны преступления, предусмотренного ст. 274.1 УК РФ. Суть правовой оценки здесь в том, что критическая инфраструктура защищается не только от активных атакующих действий, но и от эксплуатационных нарушений, когда обязанное лицо, располагая возможностью поддерживать должный уровень защищенности, не предпринимает необходимых организационно-технических шагов [7]. В плоскости доказательств ключевыми становятся наличие установленной обязанности по обновлению, реалистичность ее исполнения в конкретный момент и связь между бездействием и повышением уязвимости объектов КИИ.

Заключение. Статья 274.1 УК РФ формирует многослойную уголовно-правовую защиту критической информационной инфраструктуры, сочетая формальные составы, ориентированные на пресечение неправомерного воздействия на стадии подготовки и доступа, с материальным составом, учитывающим последствия нарушений эксплуатационной дисциплины. В центре внимания остаются ключевые параметры безопасности цифровых систем - доступность, целостность и конфиденциальность, а также непрерывность функционирования телекоммуникационных и управленческих компонентов. Такой подход позволяет реагировать на широкий спектр угроз, от целенаправленного создания и внедрения вредоносных средств до недобросовестной или небрежной эксплуатации, при этом учитывая особую общественную опасность любых посягательств в отношении инфраструктур, от стабильности которых зависят государственные функции и жизненно важные сервисы.

Список литературы

1. Бегишев, И. Р. Безопасность критической информационной инфраструктуры Российской Федерации / И. Р. Бегишев // Безопасность бизнеса. – 2019. – № 1. – С. 27-32. – EDN YSOBEL.

2. Дремлюга Р.И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение. Ср. Уголовное право. М.: Юрилитинформ, 2022. 328 с.

3. Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. … д-ра юрид. наук: 12.00.08. Москва, 2021. 557 с.

4. Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография / [П.В. Агапов и др.]; Акад. Ген. прокуратуры Рос. Федерации. М., 2014. 136 с.

5. Шутова А.А. Содержание понятия «цифровые технологии», применяемого в системе здравоохранения // Российский следователь. 2025. № 4. С. 45-49.

6. Шутова А.А. Проблемы обеспечения безопасности цифровой инфраструктуры системы здравоохранения уголовно-правовыми средствами // Безопасность бизнеса. 2025. № 1. С. 52-57.

7. Begishev I., Shutova A., Niyozmeov D., Kiiko D., Gilmanov R. Humans and Robots Transformations of Professional Communication in the Digital Era // В сборнике: 2025 Communication Strategies in Digital Society Seminar (ComSDS). IEEE, 2025. С. 144-148.

УДК 343.3/.7

С. Ю. Захарян,
соискатель кафедры уголовного права и процесса
Казанского инновационного университета
имени В.Г. Тимирясова

Последствия организации деятельности по незаконной передаче абонентских номеров с нарушением требований законодательства Российской Федерации (статья 274^4 УК РФ)

Аннотация. В представленной публикации исследуются последствия организации деятельности по незаконной передаче абонентских номеров с нарушением требований законодательства российской федерации (статья 274^4 УК РФ). Формулируются выводы о формальной конструкции состава преступления, моменте окончания преступления, особенностях установления причинно-следственной связи при опосредованном причинении вреда охраняемым общественным отношениям.

Ключевые слова: объективная сторона, ст. 274^4 УК РФ, организация деятельности, передача абонентских номеров, бланкетная диспозиция, формальный состав, участие в деятельности, законодательство о связи, незаконная деятельность

S. Y. Zakharyan,
Candidate of the Department of Criminal Law and Procedure
Kazan Innovative University
named after V.G. Timiryasov

Consequences of organizing activities on the illegal transfer of subscriber numbers from violation of the requirements of the legislation of the Russian Federation (article 274^4 of the Criminal Code of the Russian Federation)

Annotation. The presented publication examines the consequences of organizing activities for the illegal transfer of subscriber numbers in violation of the requirements of the legislation of the Russian Federation (Article 274^4 of the Criminal Code of the Russian Federation). Conclusions are formulated about the formal structure of the corpus delicti, the moment of the end of the crime, and the specifics of establishing a cause-and-effect relationship in the indirect infliction of harm to protected public relations.

Keywords: objective side, Article 274^4 of the Criminal Code of the Russian Federation, organization of activities, transfer of subscriber numbers, form disposition, formal composition, participation in activities, legislation on communications, illegal activities

Введение. Несмотря на формальную конструкцию состава преступления, предусмотренного ст. 274^4 УК РФ, исследование последствий и причинной связи сохраняет теоретическое и практическое значение.

Теоретическое значение обусловлено тем, что любое преступление по своей природе является общественно опасным деянием [2,3], а общественная опасность проявляется в способности причинять вред или создавать угрозу причинения вреда охраняемым общественным отношениям. Следовательно, даже при **формальной конструкции состава преступление объективно порождает определенные последствия, хотя они и не включены законодателем в число обязательных признаков состава** [1].

Практическое значение анализа последствий связано с тем, что характер и размер фактически причиненного вреда учитываются при назначении наказания, при решении вопросов о малозначительности деяния, при квалификации по совокупности с иными преступлениями.

Основная часть. Последствия организации деятельности по незаконной передаче абонентских номеров носят многоуровневый характер.

Первичные последствия заключаются в нарушении установленного порядка оборота абонентских номеров, подрыве системы идентификации абонентов, создании массива номеров, фактические пользователи которых не установлены или установлены неверно. Данные последствия носят организационно-правовой характер и проявляются в дезорганизации регулируемой сферы общественных отношений.

Вторичные последствия связаны с использованием незаконно переданных номеров для совершения иных преступлений: мошенничеств, неправомерного доступа к компьютерной информации, распространения противоправного контента, вымогательств, угроз. Эти последствия носят имущественный, организационный, моральный характер и затрагивают широкий круг потерпевших. Некоторые последствия проявляются на социальном уровне: подрыв доверия населения к безопасности дистанционных сервисов, снижение готовности граждан использовать цифровые финансовые инструменты, рост социальной напряженности, издержки общества на противодействие киберпреступности.

Причинная связь между организацией деятельности по незаконной передаче номеров и вторичными последствиями (конкретными преступлениями, совершенными с использованием этих номеров) носит опосредованный характер. Организатор деятельности создает инфраструктуру, обеспечивающую доступ неустановленных лиц к абонентским номерам, однако решение о совершении конкретного преступления с использованием номера принимается другим лицом (конечным пользователем номера), которое и выступает непосредственным причинителем вреда. Тем не менее, с криминологической точки зрения, организация деятельности по незаконной передаче номеров является необходимым условием множественных последующих преступлений: без доступа к анонимизированным номерам преступники оказываются лишены ключевого инструмента дистанционной преступной деятельности. Данная опосредованная причинная связь объясняет высокую общественную опасность деяния,

предусмотренного ст. 274^4 УК РФ, и обосновывает целесообразность его криминализации.

Вместе с тем опосредованный характер причинной связи между организацией передачи номеров и последствиями конкретных преступлений означает, что ответственность организатора (участника) деятельности по ст. 274^4 УК РФ не зависит от наступления данных последствий и не требует их доказывания. Если установлен факт организации (участия в) деятельности по незаконной передаче номеров, совершенной из корыстной заинтересованности или в целях совершения иного преступления, состав преступления по ст. 274^4 УК РФ является оконченным независимо от того, были ли переданные номера реально использованы для совершения иных преступлений, наступили ли какие-либо вредные последствия для конкретных потерпевших. Вместе с тем, если такие последствия наступили и доказана связь между деятельностью обвиняемого и конкретными преступлениями, это учитывается при назначении наказания как показатель степени реализации общественной опасности деяния [4].

В случаях, когда организатор (участник) деятельности по передаче номеров одновременно выступает организатором, подстрекателем или пособником конкретных преступлений, совершаемых с использованием переданных номеров, его действия требуют квалификации по совокупности преступлений: по ст. 274^4 УК РФ за организацию (участие в) деятельности по передаче номеров и по соответствующим статьям Особенной части УК РФ, предусматривающим ответственность за организацию, подстрекательство или пособничество в совершении конкретных преступлений (мошенничества, неправомерного доступа и т.д.), со ссылкой на соответствующую часть ст. 33 УК РФ. Такая квалификация обеспечивает полную правовую оценку содеянного и соответствует принципу справедливости, требующему, чтобы наказание соответствовало характеру и степени общественной опасности совершенных преступлений.

Заключение. Диспозиция ст. 274^4 УК РФ носит бланкетный характер, требуя для квалификации установления конкретных требований законодательства о связи, которые были нарушены при передаче номеров.

Состав преступления является формальным, оконченным с момента начала функционирования организованной системы передачи номеров (для организации) или с момента совершения первого действия в рамках деятельности (для участия). Не требуется наступления общественно опасных последствий в виде использования переданных номеров для совершения иных преступлений, причинения вреда конкретным потерпевшим, хотя такие последствия учитываются при назначении наказания и могут обусловливать квалификацию по совокупности с иными составами преступлений.

Список литературы

1. Новокшонов, Д. В. Объективная сторона преступления (окончание) / Д. В. Новокшонов, Н. А. Петухов, В. М. Шеншин // Аграрное и земельное право. – 2024. – № 3(231). – С. 331-334. – DOI 10.47643/1815-1329_2024_3_331. – EDN JZOVDA.

2. Реутская, Е. А. Общественная опасностькак основополагающий признак преступления / Е. А. Реутская // Борьба с преступностью: теория и практика : Тезисы докладов XII Международной научно-практической конференции. Научное электронное текстовое издание, Могилевский институт МВД, 19 апреля 2024 года. – Могилев: Могилевский институт МВД Республики Беларусь, 2024. – С. 61-63. – EDN ECNGEA.

3. Руткевич, В. Н. От общественно опасного деяния к преступлению / В. Н. Руткевич // Актуальные вопросы режима и оперативно-розыскной деятельности в уголовно-исполнительной системе : Сборник материалов круглого стола с международным участием, Псков, 26 апреля 2019 года. – Псков: Псковский филиал Академии ФСИН России, 2019. – С. 111-115. – EDN ZBBUCS.

4. Рыбак, А. З. Преступность общественно опасных деяний с учетом поведения лица до, во время и после их совершения: правоприменительный аспект / А. З. Рыбак // Юристъ-Правоведъ. – 2012. – № 6(55). – С. 42-45. – EDN QZANDH.

УДК 343.3/.7

С. Ю. Захарян,
соискатель кафедры уголовного права и процесса
Казанского инновационного университета
имени В.Г. Тимирясова

К вопросу о предмете преступления, предусмотренного статьей 274[4] УК РФ

Аннотация. В статье рассматривается специфический и новый для уголовного права предмет преступления – абонентские номера. Последние изучаются как специфические объекты гражданских прав, их правовая природа и значение в системе цифровой идентификации. Установление ответственности за организацию деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации, представляет собой закономерный этап развития отечественного правотворчества, направленного на противодействие киберпреступности.

Ключевые слова: объект преступления, ст. 274[4] УК РФ, абонентские номера, компьютерная информация, телекоммуникационные преступления, предмет преступления, цифровая идентификация, информационная безопасность

S. Y. Zakharyan,
Candidate of the Department of Criminal Law and Procedure
Kazan Innovative University
named after V.G. Timiryasov

On the issue of the subject of the crime provided for in article 274[4] of the Criminal Code of the Russian Federation

Annotation. The article considers a specific and new subject of crime for criminal law – subscriber numbers. The latter are studied as specific objects of civil rights, their legal nature and significance in the digital identification system. The establishment of responsibility for the organization of activities for the transfer of subscriber numbers in violation of the requirements of the legislation of the Russian Federation is a natural stage in the development of domestic law-making aimed at countering cybercrime.

Keywords: object of crime, Article 274[4] of the Criminal Code of the Russian Federation, subscriber numbers, computer information, telecommunication crimes, subject of crime, digital identification, information security

Введение. Введение Федеральным законом от 31 июля 2025 г. № 282-ФЗ [1] статьи 274[4] в Уголовный кодекс Российской Федерации [3] (далее – УК РФ), устанавливающей ответственность за организацию деятельности по передаче абонентских номеров с нарушением требований законодательства Российской

Федерации, представляет собой закономерный этап развития отечественного правотворчества, направленного на противодействие киберпреступности. Вместе с тем, как и любое расширение сферы уголовной репрессии, данная законодательная новелла требует всестороннего научного осмысления с позиций социальной обусловленности установления уголовной ответственности за совершение подобных деяний [4. С. 109].

Специфичен предмет преступления, предусмотренный ст. 274^4 Уголовного кодекса Российской Федерации (далее – УК РФ) – это абонентские номера, правовая природа которых является комплексной, сочетающей элементы вещного права (SIM-карта как материальный носитель), обязательственного права (права и обязанности по договору об оказании услуг связи), информационного права (номер как цифровой идентификатор).

Основная часть. Предмет преступления, предусмотренного ст. 274^4 УК РФ, составляют абонентские номера, выделенные лицам на основании договоров об оказании услуг подвижной радиотелефонной связи или предоставленные в пользование в рамках указанных договоров. Правовая природа абонентских номеров является комплексной и требует анализа с позиций различных отраслей права – гражданского, информационного, телекоммуникационного. Согласно ст. 44 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» [2] абонентский номер представляет собой «код, который используется для идентификации оконечного оборудования или пользовательского оборудования в сети подвижной радиотелефонной связи и применяется для маршрутизации сообщений и вызовов к соответствующему оборудованию». Абонентский номер не принадлежит на праве собственности ни абоненту, ни оператору связи, а входит в состав национального ресурса нумерации, который является ограниченным ресурсом Российской Федерации и находится в федеральной собственности.

Вместе с тем абонент на основании договора об оказании услуг подвижной радиотелефонной связи приобретает право пользования выделенным ему номером, которое является имущественным правом и может быть объектом гражданского оборота в установленных законом пределах. Данное право включает возможность использовать номер для осуществления и приема вызовов, отправки и получения сообщений, доступа к услугам передачи данных, регистрации в информационных системах, идентификации и аутентификации в цифровых сервисах. Абонент может сохранять право пользования номером при смене оператора связи (переносимость номера), может приостанавливать и возобновлять пользование, передавать право пользования номером иному лицу в порядке, предусмотренном законодательством и договором. Физическим носителем, обеспечивающим техническую возможность использования номера, выступает SIM-карта (модуль идентификации абонента) – смарт-карта, содержащая идентификационную информацию, ключи шифрования, программное обеспечение, обеспечивающее аутентификацию абонента в сети оператора.

С точки зрения уголовного права предметом преступления выступает не сам номер как таковой (поскольку это нематериальный объект – последовательность цифр), а право пользования номером в его неразрывной связи с физическим носителем (SIM-картой) и возможностью использования номера для доступа к услугам связи и иным сервисам. Незаконная передача номера может осуществляться в различных формах: выделение нового номера лицу, не прошедшему надлежащую идентификацию; регистрация номера с использованием документов подставных лиц, умерших граждан, поддельных документов; переоформление ранее зарегистрированного номера на иное лицо с нарушением процедур; перевыпуск SIM-карты с сохранением номера и передача ее лицу, не являющемуся законным правообладателем; предоставление виртуальных номеров, не привязанных к конкретному абоненту; использование технологий IP-телефонии для создания номеров, имитирующих номера подвижной связи, но фактически не зарегистрированных в установленном порядке.

Законодатель в диспозиции ст. 274^4 УК РФ конкретизирует предмет, указывая, что речь идет об абонентских номерах, выделенных или предоставленных в пользование на основании договоров об оказании услуг подвижной радиотелефонной связи. Данное уточнение исключает из сферы действия нормы номера фиксированной телефонной связи, виртуальные номера, не связанные с договорами подвижной связи, иные идентификаторы. Такое ограничение предмета обусловлено тем, что именно номера мобильной связи выступают в современной практике основным инструментом цифровой идентификации и наиболее часто используются в преступных целях. Номера фиксированной связи имеют меньшее криминогенное значение в силу их привязки к конкретному месту установки оборудования, меньшей универсальности использования для доступа к цифровым сервисам. Вместе с тем развитие технологий может потребовать в будущем расширения предмета преступления на иные виды телекоммуникационных идентификаторов.

Важным признаком предмета является его принадлежность: законодатель указывает, что предметом выступают номера, выделенные «лицам» (то есть законным абонентам) на основании договоров, которые затем незаконно передаются «иным лицам». Данная конструкция подчеркивает, что уголовно наказуемой является именно передача номера лицу, не имеющему законных оснований для его использования, в обход установленных процедур.

Если номер первоначально выделяется лицу с соблюдением всех требований законодательства, но затем данное лицо само использует номер в противоправных целях, состав преступления по ст. 274^4 УК РФ отсутствует (хотя могут иметь место иные составы в зависимости от характера совершаемых деяний). Состав образует именно организация системы, при которой номера регулярно выделяются или передаются лицам, не прошедшим идентификацию или использующим чужие данные, создавая тем самым ресурс анонимизированных номеров для криминального использования.

Заключение. Предмет преступления составляют абонентские номера подвижной радиотелефонной связи в их неразрывной связи с правом пользования и физическим носителем.

Список источников

1. Федеральный закон от 31 июля 2025 г. № 282-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2025. № 31. Ст. 4636.

2. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // Российская газета, 10 июля 2003 г.

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации.1996. № 25. Ст. 2954.

4. Захарян С. Ю. Основания криминализации и социальная обусловленность организации деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации // Проблемы права. 2025. № 4 (100). С. 108–118.

УДК 343.01

Л. В. Иванова,
кандидат юридических наук, доцент,
Тюменский государственный университет

Особенности уголовной ответственности соучастников киберпреступлений в эпоху искусственного интеллекта

Аннотация. В статье анализируются особенности соучастия в киберпреступлениях с учетом появления технологий искусственного интеллекта. Выделяются такие признаки, как возможность территориальной рассредоточенности соучастников, анонимность, трансформация субъективной связи между соучастниками. Автор обращает внимание на различный подход законодателя к дифференциации ответственности по формам соучастия применительно к преступлениям в сфере компьютерной информации. Рассматривается возможность соучастия человека и искусственного интеллекта. Отмечается, что современное развитие моделей искусственного интеллекта не позволяет рассматривать их субъектами преступления в силу отсутствия свободной воли и сознания.

Ключевые слова: киберпреступление, соучастие, ответственность, искусственный интеллект, группа, дифференциация, информационные технологии, цифровые технологии

L. V. Ivanova,
Candidate of Law, Associate Professor,
University of Tyumen,

FEATURES OF CRIMINAL LIABILITY OF COMPLICANTS OF CYBER CRIMES IN THE ERA OF ARTIFICIAL INTELLIGENCE

Abstract. The article analyzes the features of complicity in cybercrimes, taking into account the emergence of artificial intelligence technologies. It highlights such features as possibility of territorial dispersion of accomplices, anonymity, and transformation of subjective connections between accomplices. The author draws attention to different approaches of the legislator to the differentiation of liability for different forms of complicity in relation to computer crimes. The article examines the possibility of human and artificial intelligence complicity. It notes that the current development of artificial intelligence models does not allow them to be considered subjects of a crime due to the absence of free will and consciousness.

Keywords: cybercrime, complicity, responsibility, artificial intelligence, group, differentiation, information technology, digital technology

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

Введение. Современный уровень развития цифровых технологий выводит на новый уровень и преступную деятельность. Появление виртуальных помощников, ботов, систем, наделенных искусственным интеллектом, облегчает совершение противоправного деяния, позволяет совершать преступления в одном месте, физически находясь при этом в другом городе или даже стране, сохранять анонимность, привлекать к совершению преступления множество лиц и т.п. Данные обстоятельства свидетельствуют о повышенной общественной опасности преступлений, совершаемых с использованием информационных технологий. Для краткости будем называть такие преступления как «киберпреступления», хотя в научной литературе встречаются различные термины для таких деяний [2. С. 27]. В обобщенном виде все киберпреступления можно разделить на две большие группы: специальные киберпреступления (преступления в сфере компьютерной информации, ответственность за которые предусмотрена в гл. 28 УК РФ) и общеуголовные киберпреступления (в которых использование информационно-телекоммуникационных сетей является конструктивным или квалифицирующим признаком и ответственность за которые предусмотрена в иных главах и разделах УК РФ) [2. С. 25–33]. При этом использование при совершении преступлений моделей, наделенных искусственным интеллектом, не называется отдельно в нормах уголовного законодательства.

Основная часть. Соучастие в киберпреступлениях возможно в двух основных формах: сложного соучастия (соучастия с разделением ролей), включающего исполнителя, организатора, подстрекателя, пособника, а также простого соучастия (соисполнительства). Соучастие так же, как и цифровые технологии, повышает общественную опасность деяния в силу вредоносности и прецедентности совместного деяния [4. С. 233]. Информационные технологии играют ключевую роль в групповых преступлениях, обеспечивая координацию действий соучастников до или в ходе совершения деяния, либо выступая инструментом для достижения преступной цели.

Цифровизация преступного мира неминуемо влияет и на институт соучастия в преступлении. Представляется возможным выделить некоторые особенности ответственности соучастников в киберпреступлениях в эпоху цифровизации и искусственного интеллекта.

Прежде всего необходимо рассмотреть, каким образом уголовный закон дифференцирует ответственность за киберпреступления по формам соучастия. Учитывая, что общеуголовные киберпреступления располагаются в разных главах, остановимся только на преступлениях в сфере компьютерной информации. Обращает на себя внимание, что в рамках одной главы законодатель по-разному подходит к вопросу усиления ответственности за совершение деяния группой лиц по предварительному сговору и организованной группой. Так, в статьях 272, 273 УК РФ

ответственность не дифференцируется по формам соучастия: за совершение противоправного деяния и группой лиц по предварительному сговору, и организованной группой, предусмотрено наказание до пяти лет лишения свободы. Аналогично в ст. 274.1 УК РФ, с наказанием от трех до восьми лет лишения свободы. В других статьях данной главы наказание соучастников дифференцируется по двум формам соучастия. Так, в ст. 272.1 УК РФ за деяние, совершенное группой лиц по предварительному сговору, наказание составляет до шести лет лишения свободы, а за совершенное организованно группой – до десяти лет лишения свободы. По формам соучастия наказание дифференцируется и в ст. 274.2 УК РФ: до пяти и до шести лет лишения свободы соответственно. Представляется недопустимым различный подход законодателя к оценке общественной опасности киберпреступлений, совершаемых одним и тем же групповым способом, тем более в рамках одной главы.

Среди особенностей соучастия в эпоху цифровизации выделяется отсутствие территориального единства в местонахождении соучастников преступления (иногда соучастники могут находиться в разных странах и при этом действовать совместно), гибридный характер совершаемых действий (часть соучастников действует очно, часть дистанционно, что выводит на первый план технологические компетенции соучастников), анонимность, постоянное совершенствование киберпространства [3. С. 375–376], что позволяет совершать самые разнообразные преступления и создает сложности в части их выявления и раскрытия правоохранительными органами.

Кроме этого, спорным моментом является трансформация субъективной связи при соучастии. Отмечается, что в интернет-пространстве сложно соблюдать двустороннюю связь между соучастниками. Анонимность и территориальная рассредоточенность участников преступной деятельности позволяет говорить о возможности односторонней субъективной связи. Минимальная субъективная связь может присутствовать в цифровом пространстве между участниками организованной группы, когда, например, между руководящим звеном и непосредственными исполнителями осуществляется бесконтактное взаимодействие. Такая ситуация позволяет организатору, в случае задержания исполнителя, оставаться неустановленным для правоохранительных органов, о чем свидетельствует судебная практика, особенно по наркопреступлениям. Кроме этого, сами по себе киберпреступные группы обладают общественной опасностью, но по своим признакам не всегда могут подпадать под признаки преступных групп, ответственность за создание и участие в которых установлена в Особенной части УК РФ. Поэтому справедливо учеными предлагается закрепить самостоятельную уголовную ответственность, например, за создание хакерского сообщества и участие в нем [1. С. 102–103].

Анализируя особенности соучастия в эпоху искусственного интеллекта, нельзя не затронуть вопрос о возможности наличия соучастия с искусственным интеллектом как субъектом преступления. Зарубежные исследователи, выступающие сторонниками самостоятельной ответственности искусственного интеллекта, допускают возможность

наличия сговора и соучастия между человеком и системой ИИ, отмечая, что они могут взаимодействовать как соисполнители или иные соучастники [5. С. 78]. А способность таких систем анализировать и принимать точные решения уже свидетельствуют о наличии у них "mens rea" [6. С. 10]. Вместе с тем, на данный момент развития информационных технологий за любыми действиями систем искусственного интеллекта стоит человек, будь это разработчик (группа разработчиков), тестировщик, оператор, пользователь и т.д. И в настоящее время модели с искусственным интеллектом нельзя рассматривать самостоятельными субъектами преступлений, как минимум, из-за того, что такой подход не соответствует действующему законодательству. Кроме этого такие модели пока не обладают свободным сознанием и свободной волей (существующих не под влиянием действий человека), т.е. необходимыми субъективными компонентами для того, чтобы отдавать отчет своим действиям.

Заключение. Для соучастия в киберпреступлениях характерно широкое использование информационных технологий во взаимодействии соучастников, территориальная рассредоточенность, анонимность и как следствие, минимизация двухсторонней субъективной связи между соучастниками. Зарубежными исследователями рассматривается возможность соучастия человека и искусственного интеллекта, однако отсутствие свободной воли и сознания у современных моделей искусственного интеллекта препятствует признанию последних полноправными субъектами преступлений.

Список литературы

1. Бегишев И. Р., Хисамова З. И., Никитин С. Г. Организация хакерского сообщества: криминологический и уголовно-правовой аспекты // Всероссийский криминологический журнал. 2020. Т. 14. № 1. С. 96-105.

2. Иванова Л. В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25-33.

3. Милкина Е. В., Железогло М. Г. Особенности института соучастия в преступлении в условиях развития цифровой среды // Современный ученый. 2025. № 4. С. 373-379.

4. Шеслер А. В. Криминологические основания уголовной наказуемости за соучастие в преступлении // Всероссийский криминологический журнал. 2025. Т. 19. № 3. С. 231-244.

5. Hallevy G. The Basic Models of Criminal Liability of AI Systems and Outer Circles // Legal Aspects of Autonomous Systems / Eds. D. Moura Vicente, R. Soares Pereira, A. Alves Leal. Cham: Springer, 2024. Pp. 69-83. https://doi.org/10.1007/978-3-031-47946-5_5.

6. Mahardhika V., Astuti P., Mustafa A. Could Artificial Intelligence be the Subject of Criminal Law? // Yustisia Jurnal Hukum. 2023. Vol. 12. № 1. Pp. 1-12. https://doi.org/10.20961/yustisia.v12i1.56065.

УДК 343.275

Т. Г. Каракулов,
председатель суда,
Чаинский районный суд Томской области

Назначение уголовного наказания в виде лишения специального, воинского или почетного звания, классного чина и государственных наград в условиях цифровой трансформации общества

Аннотация. В статье автором с помощью формально-юридического и догматического методов, а также общенаучных методов анализа и синтеза, дедукции и индукции выявляются основания назначения уголовного наказания в виде лишения специального, воинского или почетного звания, классного чина и государственных наград, предусмотренного в качестве дополнительного карательного средства в ст. 48 УК РФ. Автором предложены меры, способствующие обоснованному применению этого наказания с использованием передовых технических достижений для установления юридически значимых обстоятельств о личности виновного и условиях жизни его семьи. Отмечается важная роль системы межведомственного электронного взаимодействия, функционирующей в судах общей юрисдикции и применение в судах программно-технического комплекса, обеспечивающего информационное взаимодействие ГАС «Правосудие» с аналогичными продуктами иных ведомств и государственных структур.

Ключевые слова: назначение уголовного наказания, лишение специального, воинского или почетного звания, классного чина, государственных наград, цифровые технологии, сервисы межведомственного электронного взаимодействия

T.G. Karakulov,
Chairman of the
Chainsky District Court of the Tomsk region

The imposition of criminal punishment in the form of deprivation of a special, military or honorary title, class rank and state awards in the conditions of digital transformation of society

Abstract. In the article, the author uses formal legal and dogmatic methods, as well as general scientific methods of analysis and synthesis, deduction and induction to identify the grounds for imposing criminal punishment in the form of deprivation of a special, military or honorary title, class rank and state awards, provided as an additional punitive measure in art. 48 of the Criminal Code of the Russian Federation. The author suggests measures that promote the reasonable application of this punishment using advanced technical achievements to establish legally significant circumstances about the identity of the perpetrator and the living conditions of his family. The important role of the interdepartmental

electronic interaction system operating in courts of general jurisdiction and the use of a software and hardware complex in courts that ensures information interaction between GAS «Justice» and similar products of other departments and government agencies is noted.

Keywords: imposition of criminal punishment, deprivation of a special, military or honorary title, class rank, state awards, digital technologies, interdepartmental electronic interaction services

Введение. В отличие от уголовного закона, действовавшего на рубеже XIX-XX веков (имеются в виду Уложение о наказаниях уголовных и исправительных 1845 года и Уголовное уложение 1903 года), ныне Уголовный кодекс Российской Федерации 1996 года говорит о возможности лишения виновного имеющихся у него специального и воинского звания, почетного звания и классного чина, а также присвоенных ему государственных наград не во всех случаях вынесения обвинительного приговора. Однако, с недавнего времени назначение указанного уголовного наказания в порядке применения статьи 48 Уголовного Кодекса Российской Федерации (далее – УК РФ), возможно за преступления любой категории тяжести и даже за совершение неосторожных преступных деяний.

Основная часть. В случае совершения преступных деяний повышенной общественной опасности уголовный закон для назначения наказания в виде лишения специального, воинского, почетного звания, классного чина, государственных наград исходит лишь из категории преступного деяния, которое должно быть тяжким или особо тяжким

Возможность применения такого наказания при осуждении за менее тяжкие преступные деяния существует для определенных составов преступлений, специально указанных в ст. 48 УК РФ. Из преступных деяний средней тяжести это, например, ч. 1 ст. 280^4; ч. 1 ст. 282; ст. 282^4; ч. 1 и 2 ст. 284^1; ст. 284^3; ч. 2 ст. 354^1 УК РФ, из преступных деяний небольшой тяжести два состава, предусмотренные ст. 284^2 и ч. 1 ст. 354^1 УК РФ.

Кроме категории преступления или специально поименованных составов преступлений, статья 48 УК РФ предписывает при назначении указанного уголовного наказания принимать во внимание данные о личности виновного.

В актах официального разъяснения уголовного закона в дополнение к этому указывается и на необходимость учета других, указанные в статье 60 УК РФ, обстоятельств, а это наряду с характером и степенью общественной опасности содеянного и личность подсудимого, и наказательные обстоятельства, предусмотренные ст. 61, 63 УК РФ, и уровень влияния наказания как на исправление преступника, так и на условия жизни его семьи [2], что согласуется с доктринальными положениями о необходимости учета таких данных исходя из закрепленных целей наказания [3. С. 88].

По смыслу закона характер общественной опасности преступного деяния обозначен уголовным законом и поставлен в зависимость от конкретных признаков

состава вредоносного деяния, направленного на определенные охраняемые уголовным законом социальные ценности (блага) и обычно причиняемого таким деянием вреда [2].

Как видно из нормы уголовного закона, сконструированной в ст. 48 УК РФ, при решении вопроса о назначении предусмотренного ею наказания при осуждении за совершение деяний, отнесенных к категории тяжкого или же особо тяжкого преступления, акцент в виду тяжести содеянного делается как на охраняемые общественные отношения и блага, так и на причиненный преступным деянием вред (либо существенную угрозу причинения такого вреда).

В отношение менее тяжких преступлений, за совершение которых возможно лишить звания, чина или награды на первый план выходят охраняемые уголовным законом социальные ценности, на что указывает анализ составов преступлений, специально указанных в ст. 48 УК РФ. Так, уголовное наказание, предусмотренное указанной нормой, с конца февраля 2024 года назначается и за ряд преступлений средней и небольшой тяжести, о которых мы указывали выше, к их числу относятся:

публичные призывы к осуществлению экстремистской деятельности и действий, направленных на нарушение территориальной целостности России, деятельности, направленной против безопасности России, призывы к ограничительным мерам в отношении России, ее граждан или юридических лиц;

оказание содействия в уголовном преследовании должностных лиц органов публичной власти Российской Федерации;

публичное распространение заведомо ложной информации об использовании Вооруженных Сил РФ, неоднократные пропаганда либо публичная демонстрация нацистской, экстремистской и другой запрещенной атрибутики (символики),

публичные действия, дискредитирующие использование Вооруженных Сил РФ, действия, направленные на возбуждение ненависти либо вражды, унижение достоинства человека,

осуществление деятельности нежелательной иностранной или международной организации, реабилитация нацизма.

Поскольку указанные преступные деяния посягают на безопасность государства и конституционный строй, внесение таких составов в ст. 48 УК РФ продиктовано особой важностью охраняемого объекта (объектов) в современных условиях при проведении Россией специальной военной операции.

В отличие от характера общественной опасности преступного деяния степень такой опасности коррелируется с конкретными обстоятельствами содеянного: формой вины, видом соучастия, способом совершения, преступными последствиями, наказательными обстоятельствами, относящимися к содеянному [2].

Характеризуя деятеля, суды, как правило, учитывают данные об его семейном и имущественном положении, состоянии здоровья, поведении в быту, детях и иных лиц, находящихся на иждивении.

В качестве примера учета «влияния назначенного наказания на исправление осужденного и на условия жизни его семьи» в актах официального разъяснения уголовного закона приводятся те обстоятельства, которые связаны с возможной утратой членами семьи осужденного средств к существованию в силу возраста и состояния здоровья [2].

При решении вопроса о лишении звания, классного чина, государственных наград судом учитываются и семейное положение (зарегистрированный брак, фактические брачные отношения, воспитание и содержание детей и иных иждивенцев), и имущественное положение (наличие и размер доходов, имущества), состояние здоровья подсудимого (наличие заболеваний, в том числе препятствующих осуществлению какой-либо профессиональной или служебной деятельности), поведение в быту.

Подлежат обязательному учету все указанные обстоятельства, как положительно характеризующие личность подсудимого, так и представляющие его в негативном ключе, поскольку лишение звания, чина, награды осуществляется исключительно по усмотрению суда как специально не указанное в санкциях статей Особенной части Уголовного Кодекса РФ. Сколь скоро суд в силу закона обязан мотивировать принятое решение по всем вопросам, относящимся к назначению уголовного наказания, то установление указанных обстоятельств представляется важным и в тех в случаях, когда такая карательная мера не будет дополнять назначенное виновному основное наказание.

Если характер и степень общественной опасности преступного деяния зависят от положений закона и объективных обстоятельств содеянного, то данные о личности преступника и влиянии наказания на условия жизни его семьи могут быть выявлены судом только из материалов уголовного дела и доказательств, исследованных в судебном заседании.

Не редки случаи, когда имеющихся материалов дела и доказательств, представленных сторонами, явно недостаточно для принятия решения о рассматриваемом дополнительном наказании применительно к установлению данных о личности виновного и условиях жизни его семьи либо определенные сведения об этом нуждаются в дополнительной проверке.

Принимая во внимание необходимость соблюдения не только процессуальных, но и разумных сроков уголовного судопроизводства, в определенной части восполнить пробел в установлении обозначенных обстоятельств возможно путем применения сервисов системы межведомственного электронного взаимодействия.

В судах общей юрисдикции указанная система начала формироваться с 2016 года путем налаживания обмена информацией (судебными решениями) с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

ФГБУ «ИАЦ»[27] организована доработка программного изделия «Судебное делопроизводство» подсистемы «Судебное делопроизводство и статистика» ГАС «Правосудие», а также разработка сервиса, обеспечивающего передачу сведений о принятых судами решениях посредством системы межведомственного электронного взаимодействия и направлению на исполнение в единую информационную систему Роскомнадзора судебных актов в форме электронных документов.

В 2019 году проведена опытная эксплуатация специального программного обеспечения в соответствии с Регламентом информационного обмена между Роскомнадзором и судебными органами Российской Федерации в рамках первого этапа интеграции единой информационной системы ведомства и программного изделия «Судебное делопроизводство» подсистемы «Судебное делопроизводство и статистика» ГАС «Правосудие».

Так, на сегодняшний день во всех федеральных судах Томской области организована работа по формированию и направлению документов в электронном виде с использованием программно-технического комплекса, позволяющего обмениваться информацией из системы, ГАС «Правосудие» с информационными системами иных ведомств.

Количество документов, направленных федеральными судами Томской области с использованием указанного программно-технического комплекса, возрастает значительными темпами.

Применительно к установлению уже обозначенных обстоятельств о личности преступника и условиях жизни его семьи, обсуждая возможность лишения его присвоенных регалий, суд с использованием программно-технического комплекса обеспечения информационного взаимодействия ГАС «Правосудие» может запросить и оперативно получить необходимые сведения о доходах подсудимого из ФНС, о его имуществе – из Росреестра, о возбужденных в отношении него исполнительных производствах – из ФССП, а также иные, например, из МВД или Социального Фонда России.

Как мы отмечали ранее, использование цифровых технологий может быть перспективным в части установления у подсудимого соответствующих званий и наград и при исполнении наказания, предусмотренного ст. 48 УК РФ [1. С. 19].

Заключение. Изложенное позволяет утверждать, что наряду с этим, информационные технологии могут эффективно использоваться для развития программно-технического комплекса обеспечения информационного взаимодействия ГАС «Правосудие» в целях полного и достоверного установления судом обстоятельств о личности виновного и условиях жизни его семьи необходимых для принятия решения о назначении уголовного наказания в виде лишения указанных званий, чина, наград.

[27] «Информационно-аналитический центр поддержки ГАС «Правосудие»

Список литературы

1. Каракулов, Т. Г. Лишение специального, воинского или почетного звания, классного чина и государственных наград в цифровую эпоху / Т. Г. Каракулов // Вестник Южно-Уральского государственного университета. Серия: Право. 2024. Т. 24, № 3. С. 16-21. DOI 10.14529/law240303. – EDN PESWYQ.

2. Тематический сборник Постановлений Пленума Верховного Суда. Разъяснения по Уголовному кодексу. М. Изд-во: АСТ. 2025. 608 с.

3. Уткин, В.А. Проблемы теории уголовных наказаний: курс лекций. Томск: Издательский Дом Томского государственного университета. 2018. 240 с.

УДК 343

А. В. Константинов,
кандидат юридических наук, доцент,
доцент кафедры,
Российский университет транспорта

Поисково-познавательная деятельность в сети «Интернет» (OSINT) как объект уголовно-правового исследования

Аннотация. В статье анализируется феномен Open Source Intelligence (OSINT) – разведки на основе открытых источников, эволюционировавший из сферы национальной безопасности в универсальный инструментарий для различных областей общественной жизни, бизнеса и государственного управления. Подчеркивается, что, несмотря на использование исключительно общедоступной информации, стремительное развитие OSINT в условиях цифровой трансформации ставит перед правовой наукой, особенно в контексте уголовного права, ряд фундаментальных вопросов.

Ключевые слова: открытые источники информации, поисково-познавательная деятельность, OSINT, сеть «Интернет», цифровые технологии, преступления

A. V. Konstantinov,
Associate Professor of the Department of Criminal Law, Criminal Procedure and Law Enforcement Activities of the Law Institute of the Russian University of Transport
Candidate of Legal Sciences, Associate Professor

Cognitive activities on the internet (osint) as an object of criminal law research

Abstract. The article analyzes the phenomenon of Open-Source Intelligence (OSINT), which has evolved from the field of national security into a universal tool for various areas of public life, business, and public administration. It emphasizes that, despite the use of publicly available information, the rapid development of OSINT in the context of digital transformation raises a number of fundamental questions for legal science, particularly in the field of criminal law.

Keywords: open sources of information, research and educational activities, OSINT, Internet, digital technologies, crimes

Введение. Цифровая эпоха, характеризующаяся высокими темпами роста объема информации и повсеместным проникновением информационно-телекоммуникационных технологий в сферы общественной жизни, бизнеса и государственного управления, породила феномен, получивший наименование Open Source Intelligence (OSINT) – разведка на основе открытых источников. Изначально развивавшийся в структурах национальной безопасности и спецслужб, OSINT

стремительно трансформировался в универсальный инструментарий, активно используемый в журналистских расследованиях, конкурентной разведке, анализе рисков, проверке контрагентов, поиске активов, управлении репутацией и даже в правоохранительной деятельности.

Основная часть. Сущность OSINT заключается в сборе, обработке и анализе информации, полученной исключительно из общедоступных источников, с целью извлечения полезных, скрытых или неочевидных знаний. Ключевым аспектом является именно «общедоступность» источников, что, на первый взгляд, выводит данную деятельность за рамки правового регулирования, основанного на принципах защиты конфиденциальности и ограничения доступа к закрытой информации.

Вместе с тем, стремительное развитие инструментария OSINT, появление автоматизированных систем сбора и анализа данных, а также рост сложности и изощренности методов "цифрового следа" ставят перед правовой наукой и правоприменительной практикой ряд фундаментальных вопросов. Особую остроту эти вопросы приобретают в контексте уголовного права, поскольку деятельность, формально основанная на работе с открытыми данными, может:

1. Выступать в качестве «метода» или «инструмента» совершения уголовно наказуемого деяния.

2. Сама по себе, при определенных условиях и в зависимости от «способа» сбора или «цели» использования данных, потенциально содержать признаки состава преступления.

Таким образом, OSINT перестает быть исключительно технической или оперативной дисциплиной и становится объектом пристального уголовно-правового исследования. Необходимость осмысления правовой природы OSINT, определения границ его легитимности, выявления потенциальных уголовно-правовых рисков и выработки механизмов их минимизации обусловливает актуальность обозначенного вопроса.

Разделение между легитимным OSINT и потенциально незаконной деятельностью. Использование взлома, фишинга, социальной инженерии для получения доступа к «непубличной» информации, даже если она впоследствии публикуется, не является OSINT в строгом смысле, а относится к иным видам противоправной деятельности в сфере информационных технологий или против собственности/личности. Определение граней между допустимым сбором и нарушением прав требует развития нормативной базы и экспертного подхода.

Пределы допустимости сбора информации, сопряженного с риском разглашения охраняемой законом тайны, для юридического OSINT определяются следующими ключевыми принципами и ограничениями:

1. Принцип законности источника и метода сбора. Фундаментальное требование OSINT. Информация должна быть получена исключительно из источников, доступ к которым является «законным» для OSINT-специалиста или его клиента.

Методы сбора не должны нарушать законодательство России, включая нормы о несанкционированном доступе к информации (статья 272 УК РФ), нарушении тайны связи (статья 138 УК РФ), незаконном получении сведений, составляющих тайну (статья 183 УК РФ), или административные правонарушения, связанные с незаконным получением информации (статья 13.11 КоАП РФ – нарушение законодательства РФ в области персональных данных, статья 13.14 КоАП РФ – разглашение информации с ограниченным доступом). Использование методов, включающих взлом информационных систем, социальную инженерию с применением обмана, подкуп, физическое проникновение, перехват сообщений и т.п., «выходит за рамки OSINT» и является незаконным получением информации, что может повлечь ответственность, в том числе уголовную, если полученные сведения составляют охраняемую законом тайну.

2. Принцип целевого назначения и соразмерности. Сбор информации должен осуществляться для конкретной, заранее определенной и законной цели (например, due diligence контрагента, сбор доказательств для судебного спора, анализ рынка). Объем собираемой информации должен быть «соразмерен» этой цели. Недопустим сбор избыточных сведений, особенно если они потенциально могут затрагивать охраняемую законом тайну. Если в ходе законного OSINT обнаруживаются сведения, имеющие признаки охраняемой законом тайны (например, внутренний документ компании-конкурента, выложенный по ошибке на ее сайте, но помеченный грифом «Коммерческая тайна»), OSINT-специалист должен провести тщательную оценку: является ли источник действительно открытым и законным? Насколько необходимо использовать эту информацию для достижения законной цели? Использование такой информации, даже если она формально найдена в открытом доступе, может быть расценено как недобросовестное, особенно если очевидно, что ее публикация была случайной или ошибочной, и обладатель принял меры по ее защите.

3. Оценка правового статуса обнаруженной информации. Обнаружение информации в открытом источнике не означает автоматическое снятие с нее правового режима тайны, если таковой был установлен ее обладателем и защищен законом. Например, утечка государственной тайны не лишает ее статуса государственной тайны. Утечка коммерческой тайны, если обладатель принял меры защиты, также не делает ее «общедоступной» в смысле ФЗ «О коммерческой тайне» для целей «законного» использования неограниченным кругом лиц (кроме случаев, когда сам закон обязывает раскрыть такие сведения). OSINT-специалист должен оценивать не только факт доступности, но и «вероятный правовой статус» информации. Если информация имеет признаки государственной тайны, ее обработка частным лицом недопустима. Если информация имеет признаки коммерческой, служебной или иной охраняемой законом тайны, и есть основания полагать, что она попала в открытый доступ незаконно (например, источник – явно взломанный ресурс, а содержание – внутренние документы), ее использование сопряжено с высоким риском. В таких случаях,

легитимный OSINT должен ограничиться фиксацией факта обнаружения и оценкой рисков дальнейшей обработки.

4. Разграничение «общедоступной информации» и «информации, сделанной общедоступной субъектом персональных данных для распространения». Опубликованная самим субъектом (например, в социальных сетях), теперь имеет специальный режим регулирования (статья 10.1 ФЗ «О персональных данных»). Хотя эта норма напрямую не регулирует коммерческую или служебную тайну юридических лиц или государственных органов, она отражает общую тенденцию законодателя к более строгому контролю за распространением информации, даже если она формально находится в публичном поле. Это косвенно влияет на оценку «открытости» источника: если информация опубликована физическим лицом, необходимо учитывать режим персональных данных. Если информация касается юридического лица или госоргана, необходимо оценивать, не является ли она утечкой охраняемой тайны, даже если опубликована на публичном ресурсе.

5. Профессиональная этика и внутренние политики. Законодательные ограничения устанавливают лишь минимально допустимые рамки. Ответственный юридический OSINT требует соблюдения более высоких стандартов, основанных на профессиональной этике. Это включает отказ от использования информации, происхождение которой вызывает сомнения в ее законности, даже если прямой запрет на ее использование сложно доказать. Разработка и соблюдение внутренних политик по работе с конфиденциальной и потенциально защищенной информацией являются важным элементом минимизации рисков.

6. Балансирование интересов. В случаях, когда информация, найденная в открытом источнике, может потенциально затрагивать чью-то охраняемую законом тайну (например, детали финансовой деятельности конкурента, собранные из разрозненных публичных отчетов), необходимо проводить тщательный анализ и балансировать законный интерес оператора OSINT (например, клиента, заказывающего конкурентный анализ для принятия стратегических решений) и права и законные интересы субъекта информации (конкурента, чья деятельность анализируется). Законный интерес может легитимировать сбор и анализ информации из открытых источников (пункт 7 части 1 статьи 6 ФЗ «О персональных данных» – применимо, если в данных присутствуют персональные данные; по аналогии может применяться к оценке правомерности действий в отношении информации о юридических лицах), но он не может служить основанием для незаконного получения или использования информации, составляющей охраняемую законом тайну.

Таким образом, даже работа с общедоступными данными, если они содержат персональные данные, подпадает под действие ФЗ-152. Масштабный сбор (парсинг) открытых профилей, их систематизация, создание баз данных, содержащих персональные данные, без явного согласия субъекта или иного законного основания может быть квалифицировано как незаконная обработка персональных данных.

Гораздо более сложный и дискуссионный вопрос является то, что может ли сама деятельность по сбору, обработке и анализу «открытых» данных при определенных обстоятельствах содержать признаки состава преступления? Прямого запрета на OSINT в УК РФ нет. Однако отдельные действия, совершаемые в рамках OSINT или под его прикрытием, могут подпадать под статьи, криминализирующие деяния в сфере информационных технологий и против конституционных прав граждан. Особое место занимает новая статься УК РФ. Ст. 272.1 УК РФ

Заключение. В данный момент времени использование инструментов OSINT и соответственно предоставление услуг в сфере OSINT находится в ситуации правовой неопределенности и в состоянии ожидания правоприменительной практики по ст. 272.1 УК РФ. В связи с этим стоит обозначить современную востребованность, а также актуальность исследования и изучения дисциплины OSINT в контексте юридико-технического понимания.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ. // «КонсультантПлюс» (Дата обращения 12.05.2025)

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.

УДК 343.3/.7

Д. С. Корешников,
преподаватель,
Уральский государственный юридический университет
имени В. Ф. Яковлева

Таргетированная реклама в сети «Интернет»: уголовно-правовые риски в свете ст. 272.1 УК РФ

Аннотация. Анализируется механизм функционирования таргетированной (целевой) рекламы в сети «Интернет» с точки зрения соблюдения законодательства Российской Федерации о персональных данных и положений уголовной ответственности по статье 272.1 УК РФ. Обосновывается вывод о том, что использование такой рекламы связано со сбором информации, включая данные, относящиеся к категории персональных, а их последующее хранение и передача рекламодателям могут противоречить требованиям Федерального закона «О персональных данных». Отмечается, что в случае расширительного толкования такого признака состава преступления, предусмотренного статьей 272.1 УК РФ, как «неправомерный доступ к информации», существует риск криминализации всей деятельности, связанной с использованием механизмов таргетированной рекламы.

Ключевые слова: таргетированная реклама, целевая реклама, персональные данные, компьютерная информация, уголовная ответственность, право, цифровые технологии

D. S. Koreshnikov,
Lecturer,
Ural State Law University
named after V.F. Yakovlev

Targeted advertising on the internet: criminal law risks in the context of article 272.1 of the Criminal Code of the Russian Federation

Abstract. This article examines the operational mechanisms of targeted (personalized) online advertising with regard to Russian personal data legislation and the criminal law provisions set forth in Article 272.1 of the Criminal Code of the Russian Federation. The analysis demonstrates that targeted advertising inherently involves the collection, storage, and transfer of personal data, activities which may conflict with the requirements of the Federal Law “On Personal Data.” The paper critically assesses the potential for expansive interpretation of the notion of “unlawful access to information” within Article 272.1, highlighting the risk of criminalizing standard advertising practices that employ data-driven

targeting technologies. The discussion emphasizes the need for a balanced legal framework that differentiates between legitimate marketing activities and unlawful data processing.

Keywords: targeted advertising, personalized advertising, personal data, digital information, criminal liability, law, digital technologies

Введение. В настоящее время в сети «Интернет» широко используется таргетированная реклама, при функционировании которой обрабатываются персональные данные пользователей. В связи с введением в Уголовный кодекс Российской Федерации статьи 272.1 возникает вопрос: может ли деятельность по использованию механизмов таргетированной рекламы подпадать под признаки состава указанного преступления.

Основная часть. Законодательного определения понятия «таргетированная реклама» не существует, как нет и специального правового регулирования [18. С. 601–606]. Однако данный термин встречается в судебных актах [5] и широко используется в маркетинговой сфере.

Упрощенно таргетированная реклама (целевая или выборочная реклама; англ. targeted advertising) – это способ онлайн-рекламы, в котором используются методы и настройки поиска целевой аудитории в соответствии с заданными параметрами (характеристиками и интересами) людей, которые могут интересоваться рекламируемым товаром или услугой [15].

В юридической литературе отмечается широкое распространение таргетированной рекламы и предлагаются более детальные определения [8. С. 9–15; 10. С. 70–80; 13. С. 25–28; 17. С. 119–133; 18. С. 601–606], одно из которых звучит следующим образом: «Таргетированная реклама – информация, распространенная в информационно-телекоммуникационной сети «Интернет» в форме персонализированных и целенаправленных сообщений с использованием средств вычислительной техники, адресованная определенному кругу потенциальных потребителей, учитывающая их интересы и потребности и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке» [10. С. 70–80].

Пользователь сети «Интернет» сталкивается с такой рекламой регулярно. Заходя на тот или иной сайт, он видит баннеры о товарах и услугах, которые искал некоторое время назад через поисковые системы или при посещении сайтов со схожими предложениями. При этом реклама учитывает его местонахождение и предлагает товары в соответствующем населенном пункте или регионе.

Функционирование таргетированной рекламы основано на сборе и последующей обработке пользовательских данных. Часть информации люди предоставляют самостоятельно при регистрации в социальных сетях и сервисах. Другая, более значительная часть пользовательских данных, собирается с помощью технических средств: файлов cookie, идентификаторов устройств и других.

Так, при посещении интернет-сайта на устройство пользователя пересылается файл cookie, в котором хранятся сведения о том, с какого устройства он заходил, как регистрировался на сайте, какие действия совершал и т. д. [11. С. 516–531]. Браузер сохраняет этот файл в системной папке и при каждом последующем обращении к тому же сайту автоматически передает cookie обратно на сервер. Сервер читает cookie и восстанавливает пользовательские настройки, сеансы, авторизацию, содержимое корзины и другую персонализированную информацию. Существуют разные типы таких файлов. Так, first-party cookies (основные, первоначальные куки-файлы) создаются самим сайтом для запоминания предпочтений пользователя (язык, товары в корзине, авторизация), a third-party cookies (сторонние куки-файлы) устанавливаются внешними рекламными платформами и позволяют отслеживать пользователя на разных сайтах [19. С. 174–177].

Сбор пользовательских данных ведут не только владельцы сайтов, но и производители программного обеспечения, мобильных приложений, оборудования, автомобилей и даже бытовой техники (умные пылесосы, домашние колонки, смарт-телевизоры).

Все информация аккумулируются брокерами данных (Data Brokers). Брокеры покупают данные у широкого круга вышеуказанных организаций, так или иначе занимающихся сбором пользовательской информации (от владельцев сайтов до производителей программного обеспечения). При этом формируется цифровой портрет пользователя, включающий тысячи атрибутов. Крупные брокеры, такие как Acxiom и Oracle, собирают от 3 000 до 30 000 атрибутов на одного человека [16]. Данные могут быть демографическими (национальность, пол, возраст, уровень образования, экономический статус, уровень дохода), психографическими (ценности, мнения, образ жизни, интересы), поведенческими (история браузера, информация о покупках и действиях на сайтах), географическими (место жительства, место пребывания в реальном времени, геолокация), техническими (характеристики устройства, которым пользуется человек) и так далее.

Дальнейшая передача данных происходит в рамках технологии RTB (Real-Time Bidding) – аукциона рекламных объявлений в реальном времени. Этот процесс занимает менее одной секунды и выглядит следующим образом. В момент, когда пользователь загружает веб-страницу или открывает приложение, владелец данного сайта или приложения (SSP – Sell-Side Platform) отправляет запрос на показ рекламы в рекламную сеть (Ad Exchange), прилагая данные о пользователе. Рекламная биржа мгновенно рассылает эти данные всем участникам аукциона – многочисленным рекламным платформам (DSP – Demand-Side Platform). Платформы DSP обогащают полученные данные, обращаясь к платформам управления данными (DMP – Data Management Platform), которые, в свою очередь, получают информацию от брокеров данных. На основе полного портрета пользователя происходит аукцион, участники которого делают ставки. Победитель получает право показать свою рекламу. Все это

происходит за доли секунды, и в итоге пользователь получает рекламу, нацеленную именно на него. За время загрузки сайта его данные успевают передать, обогатить, выставить на аукцион и продать рекламодателю. Таким образом, пользовательские данные фактически распространяются среди множества субъектов, включая организации, находящиеся за пределами юрисдикции Российской Федерации.

Вопрос об отнесении автоматически собираемой пользовательской информации к персональным данным неоднократно вставал в правоприменительной практике.

Согласно статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон 152-ФЗ) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [1]. Ссылаясь на данное определение, надзорные органы, суды [4] и ученые [19. С. 174–177] признавали cookies и иные пользовательские данные, полученные в том числе для использования в таргетированной рекламе, персональными данными, поскольку они позволяют идентифицировать пользователя.

Сбор, хранение и передача таких данных сопровождаются рисками нарушения закона [14. С. 108–113], наиболее распространенные из которых:

– отсутствие надлежащего согласия субъекта персональных данных. Многие сайты устанавливают cookies и иным образом собирают данные без получения явного согласия пользователя, либо полученное согласие не отвечает требованиям закона о его конкретности, предметности, информированности, сознательности и однозначности (нарушение статьи 9 Закона 152-ФЗ);

– нарушение принципа локализации. Хранение и обработка данных россиян за пределами Российской Федерации с использованием зарубежных аналитических сервисов для обработки данных нарушает правила о трансграничной передаче данных (статьи 12 и 18 Закона 152-ФЗ) [3; 4; 6].

Показательным в плане нарушения законодательства при таргетированной рекламе является гражданское дело по иску к ООО «Гугл». Согласно судебному решению Московского городского суда, гражданин обратился с иском к данной компании и просил запретить ответчику чтение его личной корреспонденции. В обоснование своих требований истец указал, что является пользователем электронного почтового ящика с адресом «****@gmail.com» и при прочтении личной переписки обнаружил, что рекламные объявления, встроенные в текст письма, соответствуют содержанию электронной переписки [2].

В ходе судебного заседания по данному иску исследовалась, в частности, политика конфиденциальности продукта Google, размещенная на официальном сайте в разделе «Как мы используем собранные данные». Согласно данной политике, компания уведомляет: «…наши системы автоматически анализируют ваш контент (в т. ч. электронные письма), чтобы предоставлять функции, полезные вам. Это могут быть отобранные для вас результаты поиска, релевантные рекламные объявления,

выявление спама и вредоносных программ…». Этот документ и иные доказательства позволили судебной коллегии прийти к выводу: ООО «Гугл», исполняя обязательства перед третьими лицами по договорам размещения рекламы и ее эффективного распространения в сегменте продукта Google, проводит мониторинг электронной почты, а затем размещает рекламные сообщения в том числе и в частной переписке пользователей Российской Федерации на основании анализа информации конкретного пользователя [2]. Такие действия нарушают законодательство Российской Федерации.

Примечательно, что компанию Google привлекают к ответственности за нарушение прав пользователей при сборе информации и за пределами России. Так, 04.09.2025 жюри присяжных в Сан-Франциско (США) вынесло вердикт, согласно которому корпорация Google должна выплатить 425,7 млн. долларов по коллективному иску о нарушении права пользователей на неприкосновенность частной жизни. Как установил суд, начиная с 2016 года Google собирала данные пользователей из сторонних приложений, даже если параметр «История приложений и веб-поиска» был отключен в настройках устройств [9].

Таким образом, получение пользовательских данных для целей таргетированной рекламы может быть неправомерной и нарушать конституционные права граждан и законодательство о персональных данных.

Возникает вопрос: может ли подобная деятельность квалифицироваться по ст. 272.1 УК РФ, предусматривающей ответственность за незаконное использование, передачу, сбор или хранение компьютерной информации, содержащей персональные данные, полученной в результате неправомерного доступа либо иным незаконным способом.

Толкование данной нормы применительно к таргетированной рекламе возможно в двух направлениях.

Первый подход предполагает наличие состава преступления в действиях всех участников процесса обработки персональных данных пользователей, которые не смогут доказать правомерность этих действий. При толковании «неправомерности» в ст. 272.1 УК РФ можно исходить из презумпции незаконности нахождения у какого-либо лица чужих персональных данных, пока он не докажет обратного. Такой подход предусмотрен в ч. 3 ст. 9 Закона 152-ФЗ, согласно которой обязанность предоставить доказательство получения согласия субъекта персональных данных либо доказательство наличия иных законных оснований возлагается на оператора. В этом случае персональные данные в уголовно-правовом смысле будут схожи с таким предметом преступления, как наркотические средства: их сбыт и хранение изначально оцениваются как преступные, кроме случаев, когда лицо докажет законность владения ими. При таком подходе угрозе уголовного преследования может быть подвергнута целая отрасль. Объем российского рынка интерактивной рекламы и продвижения в Интернете в 2024 году составил 1,236 трлн руб. [7], и значительная его часть пришлась на таргетированную рекламу.

Второй подход исходит из необходимости доказывания правоохранительными органами осознания оператором того, что он обрабатывает персональные данные, полученные незаконным путем. При отсутствии доказательств такого знания состав преступления отсутствует. Этот вариант предпочтительнее, поскольку соответствует принципам уголовного права: презумпции невиновности (ст. 49 Конституции РФ, ст. 14 УК РФ) и недопустимости объективного вменения (ч. 2 ст. 5 УК РФ). Однако при таком подходе пользователь сети «Интернет» может оставаться без надлежащей правовой защиты своих персональных данных несмотря на то, что «защита частной жизни – важная часть демократии и гражданских свобод. Пользователи должны контролировать свои данные и быть защищенными от необоснованного мониторинга и киберпреступлений» [10. С. 70–80].

Таким образом, можно констатировать, что в настоящее время статья 272.1 УК РФ, в связи с отсутствием четких критериев отнесения источников происхождения компьютерной информации, содержащей персональные данные, к незаконным, позволяет избирательно применять ее к участникам отношений, связанных с таргетированной рекламой. Это противоречит принципу равенства граждан перед законом (статья 4 УК РФ).

Как отмечалось в литературе, «в сфере защиты персональных данных и частной жизни в цифровой среде фундаментальное значение имеет вопрос о балансе, взаимовыгодном компромиссе между комфортом и свободой – как субъекта персональных данных, так и оператора (юридического лица, осуществляющего предпринимательскую деятельность с использованием цифровых инструментов» [12. С. 87–102].

Заключение. Требуется уточнение состава преступления, закрепленного в ст. 272.1 УК РФ, в том числе путем закрепления критериев «незаконности получения персональных данных». Это обеспечит баланс между защитой прав граждан на неприкосновенность частной жизни и недопустимостью чрезмерной криминализации сферы цифровой рекламы.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс» [Электронный ресурс]. (дата обращения: 07.09.2025).

2. Апелляционное определение Московского городского суда от 16.09.2015 по делу N 33-30344 СПС «КонсультантПлюс» [Электронный ресурс]. (дата обращения: 07.09.2025).

3. Апелляционное определение Московского городского суда от 10.11.2016 по делу 33-38783 // СПС «КонсультантПлюс» [Электронный ресурс]. (дата обращения: 07.09.2025).

4. Постановление Второго кассационного суда общей юрисдикции от 26.12.2022 по делу № 16-9987/2022 // СПС «КонсультантПлюс» [Электронный ресурс]. (дата обращения: 07.09.2025).

5. Постановление Девятого арбитражного апелляционного суда от 13.06.2012 № 09АП-14264/2012-АК по делу № А40-112441/11-90-469 // СПС «КонсультантПлюс» [Электронный ресурс]. (дата обращения: 07.09.2025).

6. Постановление Таганского районного суда г. Москвы от 04.08.2016 по делу №2-3491/2016. // URL: https://www.mos-gorsud.ru/rs/taganskij/cases/docs/content/27b4bb17-652a-4e2f-a101-d3c82bcdf2c4 (дата обращения: 07.09.2025).

7. АРИР: Объем российского рынка интернет-рекламы впервые превысил 1 трлн рублей // URL: https://www.sostav.ru/publication/obem-rossijskogo-rynka-internet-reklamy-74596.html (дата обращения: 07.09.2025).

8. Аблятипова Н.А., Кравцова А.А. Таргетированная реклама: гражданско-правовой аспект // Крымский научный вестник. 2019. №3 (24). С. 9-15.

9. Блумберг: Google обязали выплатить $425,7 млн за нарушение конфиденциальности. // URL: https://tass.ru/ekonomika/24954573 (дата обращения: 07.09.2025).

10. Васильева Я.В., Шалегин С.П. Защита персональных данных в процессе использования таргетированной рекламы // Юридические исследования. 2024. № 6. С. 70-80.

11. Гадельшин А.А., Степанов М.М. Cookie-файлы как объект персональных данных и способ нарушения конфиденциальности персональных данных // Вопросы российской юстиции. 2021. №16. С. 516-531.

12. Геращенко А.И., Рыбин А.И., Зюбанов К.А. Защита персональных данных в эпоху надзорного капитализма // Международное правосудие. 2023. N 4 (48). С. 87-102.

13. Кряжевских К.А. Проблемы защиты персональных данных в процессе использования таргетированной рекламы // Умная цифровая экономика. 2022. №3. С. 25-28.

14. Сошнева Н.А. Таргетированная реклама и персональные данные // студенческий журнал Ex Adverso. 2022. N 1. С. 108-113.

15. Таргетированная реклама // URL: https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D1%80%D0%B5%D0%BA%D0%BB%D0%B0%D0%BC%D0%B0 (дата обращения: 07.09.2025)

16. Таргетированная реклама как инструмент шпионажа в ИБ // URL: https://rutube.ru/video/63db0cb926a34cd71422f0d20804637f/ (дата обращения: 07.09.2025).

17. Харитонова Ю.С. Контекстная (поведенческая) реклама и право: точки пересечения // Право в сфере Интернета: Сборник статей. Рук. авт. кол. и отв. ред. М.А. Рожкова. С. 119-133. // URL: https://rozhkova.com/books_text/PRAVO_internet.pdf (дата обращения: 07.09.2025).

18. Хашаева Д.А. Проблемы правового регулирования таргетированной рекламы в сети интернет // Образование и право. 2024. №3. С. 601-606.

19. Чипигина П.А. Правовое регулирование cookie // Образование и право. 2023. №6. С. 174-177.

УДК 343.3/.7

С. В. Кравчук,
соискатель кафедры уголовного права и процесса
Казанского инновационного университета
имени В.Г. Тимирясова

Установление и доказывание признаков субъективной стороны состава преступления, предусмотренного статьей 274[3] УК РФ

Аннотация. В статье проводится исследование субъективной стороны преступления, предусмотренного ст. 274[3] УК РФ, устанавливающей ответственность за незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции. Обосновывается вывод о сложной конструкции субъективной стороны, сочетающей элементы интеллектуального осознания технической природы предмета преступления, нормативного понимания незаконности деяния и целевой направленности на создание условий для совершения иных преступлений. Предложены рекомендации по методике установления и доказывания признаков субъективной стороны в процессе расследования и судебного рассмотрения уголовных дел данной категории.

Ключевые слова: субъективная сторона преступления, вина, умысел, специальная цель, мотив, двойная форма вины, юридическая ошибка, фактическая ошибка, интеллектуальный элемент умысла, волевой элемент умысла, доказывание субъективных признаков, квалификация преступлений

S. V. Kravchuk,
Candidate of the Department of Criminal Law and Procedure
Kazan Innovative University
named after V.G. Timiryasov

Establishing and proving the signs of the subjective side of the corpus delicti, provided for in article 274[3] of the Criminal Code of the Russian Federation

Annotation. The article examines the subjective side of the crime provided for in Article 274[3] of the Criminal Code of the Russian Federation, which establishes responsibility for the illegal use of a subscriber's traffic terminal or virtual telephone exchange. The author substantiates the conclusion about the complex construction of the subjective side, combining elements of intellectual awareness of the technical nature of the subject of the crime, a normative understanding of the illegality of the act and a targeted focus on creating conditions for the commission of other crimes. Recommendations on the methodology for establishing and proving signs of a subjective side in the process of investigation and judicial review of criminal cases of this category are proposed.

Keywords: subjective side of the crime, guilt, intent, special purpose, motive, double form of guilt, legal error, factual error, intellectual element of intent, volitional element of intent, proving subjective signs, qualification of crimes

Введение. Установление и доказывание признаков субъективной стороны преступления представляет одну из наиболее сложных задач в процессе расследования и судебного рассмотрения уголовных дел, поскольку субъективные психические процессы, протекающие в сознании субъекта, не поддаются непосредственному наблюдению и могут быть установлены только на основании анализа объективных обстоятельств, косвенно свидетельствующих о содержании умысла, целях и мотивах преступного поведения [1. С. 88-109]. Применительно к преступлению, предусмотренному ст. 274^3 УК РФ, доказывание субъективной стороны требует получения совокупности доказательств, подтверждающих осознание субъектом технической природы используемого оборудования, незаконности его использования, общественной опасности совершаемых действий, наличие специальной цели совершения иного преступления. Методика доказывания субъективной стороны основывается на презумпции соответствия субъективного отношения лица к совершаемым действиям их объективному характеру: если объективно действия характеризуются определенными признаками, презюмируется, что субъект осознавал эти признаки, если не доказано иное.

Основная часть. Основным источником доказательств содержания субъективной стороны выступают показания обвиняемого, в которых он излагает свое отношение к совершенному деянию, объясняет цели и мотивы своего поведения, описывает свое понимание характера используемого оборудования и осознание правовых последствий своих действий. Признательные показания обвиняемого, содержащие подробное описание субъективных элементов преступления, существенно облегчают доказывание и могут рассматриваться как смягчающее обстоятельство при назначении наказания. Вместе с тем, показания обвиняемого не могут быть единственным источником доказательств субъективной стороны и должны быть подкреплены совокупностью объективных доказательств, подтверждающих содержание умысла. Если обвиняемый отрицает наличие умысла на незаконное использование оборудования или специальной цели совершения иного преступления, ссылаясь на добросовестное заблуждение относительно правомерности своих действий, следствие обязано опровергнуть эти утверждения путем доказывания объективных обстоятельств, исключающих возможность добросовестного заблуждения.

Важным источником доказательств субъективной стороны выступают показания соучастников преступления, согласившихся на сотрудничество со следствием и дающих подробные показания о распределении ролей в преступной группе, содержании достигнутых соглашений о совместной преступной деятельности,

обсуждениях целей использования телекоммуникационного оборудования. Показания соучастников позволяют установить, что все участники преступной группы осознавали противоправный характер своей деятельности, понимали, что создаваемая техническая инфраструктура предназначена для совершения мошенничеств, и действовали с единым умыслом на достижение общей преступной цели. Показания свидетелей, не являющихся соучастниками преступления, но осведомленных об обстоятельствах дела, могут подтверждать отдельные элементы субъективной стороны: свидетели могут сообщить о высказываниях обвиняемого относительно целей использования оборудования, о переговорах с заказчиками услуг, о демонстрации осведомленности в технических характеристиках оборудования.

Важным источником доказательств субъективной стороны выступают результаты оперативно-розыскных мероприятий, прежде всего прослушивание телефонных переговоров и снятие информации с технических каналов связи, позволяющие получить объективные данные о содержании коммуникаций между участниками преступной группы, переговорах с заказчиками услуг, обсуждениях технических деталей функционирования оборудования. Содержание перехваченных переговоров может прямо свидетельствовать о наличии умысла на незаконное использование оборудования и специальной цели совершения мошенничеств, если участники обсуждают противоправный характер своей деятельности, способы уклонения от ответственности, распределение доходов от преступной деятельности. Вещественные доказательства, включая изъятое телекоммуникационное оборудование, компьютерную технику, электронные носители информации, финансовые документы, содержат объективную информацию, косвенно свидетельствующую о субъективной стороне преступления. Техническая конфигурация оборудования, специально настроенного для подмены номеров и массовых автоматизированных рассылок, свидетельствует о том, что субъект осознавал специализированное назначение оборудования и использовал его именно для создания условий совершения мошенничеств.

Заключение. Доказывание признаков субъективной стороны представляет существенную сложность для правоприменительной практики и требует получения совокупности прямых и косвенных доказательств, включающих показания обвиняемого и соучастников преступления, показания свидетелей, результаты оперативно-розыскных мероприятий, вещественные доказательства, заключения экспертов. Методика доказывания основывается на презумпции соответствия субъективного отношения лица к совершаемым действиям их объективному характеру: если объективно действия характеризуются определенными признаками, презюмируется осознание субъектом этих признаков. Техническая конфигурация оборудования, специально настроенного для подмены номеров и массовых автоматизированных рассылок, размер получаемого вознаграждения, содержание коммуникаций, проходящих через оборудование, продолжительность преступной

деятельности выступают объективными обстоятельствами, косвенно свидетельствующими о наличии умысла на незаконное использование оборудования и специальной цели совершения иных преступлений [2. С. 50-52].

Список литературы

1. Петелин, Б. Я. Установление субъективной стороны преступления в процессе расследования (теоретические и тактико-методические аспекты) / Б. Я. Петелин // Публичное и частное право. – 2009. – № 3(3). – С. 88-109. – EDN LDGQFX.

2. Рудов, Д. Н. К вопросу о расследовании преступлений, совершенных с использованием скиммингового оборудования / Д. Н. Рудов // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2016. – № 1(43). – С. 50-52. – EDN VRAPJH.

УДК 343.3/.7

С. В. Кравчук,
соискатель кафедры уголовного права и процесса
Казанского инновационного университета
имени В.Г. Тимирясова

Уголовно-правовое значение фактической и юридической ошибок при квалификации преступлений в сфере незаконного использования абонентского терминала пропуска трафика или виртуальной телефонной станции

Аннотация. В статье исследуются виды юридических и фактических ошибок, влияющих на квалификацию деяния и ответственность субъекта. Обосновывается вывод о сложной конструкции субъективной стороны состава преступления, предусматривающего ответственность за незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции (статья 274^3 УК РФ), сочетающей элементы интеллектуального осознания технической природы предмета преступления, нормативного понимания незаконности деяния и целевой направленности на создание условий для совершения иных преступлений.

Ключевые слова: субъективная сторона преступления, вина, умысел, специальная цель, мотив, двойная форма вины, юридическая ошибка, фактическая ошибка, интеллектуальный элемент умысла, волевой элемент умысла, доказывание субъективных признаков, квалификация преступлений.

S. V. Kravchuk,
Candidate of the Department of Criminal Law and Procedure
Kazan Innovative University
named after V.G. Timiryasov

The criminal and legal significance of the actual and legal errors in the qualification of crimes in the field of illegal use of a subscriber terminal for passing traffic or a virtual telephone exchange

Annotation. The article examines the types of legal and factual errors that affect the qualification of the act and the responsibility of the subject. The author substantiates the conclusion about the complex construction of the subjective side of the crime, which provides for responsibility for the illegal use of a subscriber terminal or a virtual telephone exchange (Article 274^3 of the Criminal Code of the Russian Federation), combining elements of intellectual awareness of the technical nature of the subject of the crime, a normative understanding of the illegality of the act and a targeted focus on creating conditions for the commission of other crimes.

Keywords: subjective side of the crime, guilt, intent, special purpose, motive, double form of guilt, legal error, factual error, intellectual element of intent, volitional element of intent, proving subjective signs, qualification of crimes.

Введение. Введение ст. 274^3 «Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции» в Уголовный кодекс Российской Федерации (далее – УК РФ) Федеральным законом от 31 июля 2025 г. № 282-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» [1] актуализировало необходимость доктринального исследования признаков субъективной стороны данного преступления, выявления особенностей содержания умысла, определения критериев установления специальной цели, анализа проблемы двойной формы вины. Техническая сложность предмета преступления, альтернативная конструкция объективной стороны, сочетание формального и материального составов создают специфические особенности субъективной стороны, требующие теоретического осмысления и выработки практических рекомендаций для правоприменения. Ошибка в уголовном праве представляет собой неправильное представление лица о фактических обстоятельствах совершаемого деяния или его юридических свойствах, влияющее на содержание умысла и имеющее значение для квалификации преступления, определения пределов уголовной ответственности.

Основная часть. Теория уголовного права разграничивает юридическую и фактическую ошибку [2,6,7].

Юридическая ошибка представляет собой неправильное представление лица о правовой характеристике совершаемого деяния: его преступности или непреступности, квалификации, виде и размере наказания [3, С. 272-274]. Фактическая ошибка представляет собой неправильное представление лица о фактических обстоятельствах, относящихся к объективным признакам состава преступления: об объекте посягательства, предмете преступления, характере совершаемого деяния, его последствиях, причинной связи [5, С. 332-334]. Юридическая и фактическая ошибка имеют различное уголовно-правовое значение и по-разному влияют на квалификацию деяния и ответственность субъекта.

Юридическая ошибка, как правило, не влияет на квалификацию преступления и не исключает уголовную ответственность, поскольку в основе уголовного права лежит принцип презумпции знания закона: незнание закона не освобождает от ответственности. Применительно к преступлению, предусмотренному ст. 274^3 УК РФ, возможны следующие варианты юридической ошибки:

– ошибка в преступности деяния, когда лицо ошибочно полагает, что незаконное использование абонентского терминала пропуска трафика не является преступлением и влечет только административную ответственность;

– ошибка в квалификации, когда лицо полагает, что его действия образуют иной состав преступления;

– ошибка в наказуемости, когда лицо неправильно представляет вид и размер наказания, предусмотренного за совершенное преступление.

Все указанные варианты юридической ошибки не влияют на квалификацию и не исключают уголовную ответственность. Лицо, незаконно использующее абонентский терминал пропуска трафика в целях совершения иного преступления, подлежит уголовной ответственности по ч. 1 ст. 274^3 УК РФ независимо от того, осознавало ли оно преступность своего деяния в юридическом смысле или ошибочно полагало, что совершает административное правонарушение.

Вместе с тем, в доктрине уголовного права признается, что в исключительных случаях юридическая ошибка может влиять на квалификацию, если заблуждение лица относительно правовой оценки деяния основано на объективных обстоятельствах и касается нормативных признаков состава преступления [4]. Применительно к ст. 274^3 УК РФ критически важным нормативным признаком выступает незаконность использования телекоммуникационного оборудования. Если лицо добросовестно заблуждалось относительно законности использования оборудования, имея разумные основания полагать, что деятельность осуществляется в соответствии с требованиями законодательства о связи, такое заблуждение может исключать осознание незаконности как элемент интеллектуального компонента умысла. Например, если лицо получило от недобросовестных консультантов ошибочные разъяснения о том, что для осуществляемой им деятельности не требуется получение лицензии, или было введено в заблуждение относительно наличия у организации, от имени которой оно действует, необходимых лицензий и разрешений, такое добросовестное заблуждение может исключать умысел на незаконное использование оборудования. Установление добросовестности заблуждения требует анализа всей совокупности объективных обстоятельств, свидетельствующих о наличии или отсутствии у лица разумных оснований для заблуждения.

Фактическая ошибка применительно к преступлению, предусмотренному ст. 274^3 УК РФ, может выражаться в нескольких вариантах.

Ошибка в предмете преступления имеет место, когда лицо неправильно оценивает техническую природу используемого оборудования, полагая, что оно не является абонентским терминалом пропуска трафика или виртуальной телефонной станцией. Если лицо ошибочно полагало, что используемое им оборудование представляет собой обычное офисное телекоммуникационное оборудование, не обладающее специфическими функциональными возможностями массовой автоматизированной обработки коммуникаций, и имело объективные основания для такого заблуждения, ошибка в предмете преступления исключает умысел на незаконное использование абонентского терминала пропуска трафика. Однако если объективные характеристики оборудования, его техническая конфигурация, способ использования однозначно свидетельствуют о его специализированном назначении,

ссылка субъекта на незнание технической природы оборудования не может быть признана добросовестным заблуждением и не исключает умысла.

Ошибка в последствиях имеет значение для материального варианта состава преступления, когда незаконное использование оборудования повлекло тяжкие последствия. Если лицо не предвидело возможности наступления тяжких последствий, хотя должно было и могло их предвидеть, такая ошибка могла бы свидетельствовать о неосторожной форме вины в отношении последствий. Однако, как отмечалось выше, характер тяжких последствий как закономерного результата умышленного незаконного использования специализированного оборудования в значительных масштабах делает маловероятной ситуацию неосознания возможности наступления таких последствий.

Ошибка в причинной связи, когда лицо неправильно представляет механизм причинения вреда, не влияет на квалификацию, если последствия фактически наступили и находятся в причинной связи с совершенным деянием. Ошибка в развитии причинной связи не исключает уголовную ответственность, если последствия, которые лицо предвидело и желало или допускало, фактически наступили, хотя механизм их причинения отличался от представления субъекта.

Заключение. Юридическая ошибка, как правило, не влияет на квалификацию преступления и не исключает уголовную ответственность, однако в исключительных случаях добросовестное заблуждение относительно законности использования оборудования, основанное на объективных обстоятельствах, может исключать осознание незаконности как элемент интеллектуального компонента умысла.

Фактическая ошибка в предмете преступления, когда лицо не осознавало технической природы используемого оборудования как абонентского терминала пропуска трафика, может исключать умысел при наличии объективных оснований для заблуждения.

Установление добросовестности заблуждения требует анализа всей совокупности обстоятельств, свидетельствующих о наличии или отсутствии у лица разумных оснований для ошибочного представления о фактических или юридических обстоятельствах.

Список литературы

1. Федеральный закон от 31 июля 2025 г. № 282-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета, 6 августа 2025 г.

2. Вахненко А. А., Грешнова Н. А. Доктринальные проблемы классификации уголовно-правовых ошибок // Вестник Саратовской государственной юридической академии. 2021. № 2 (139). С. 145-152. doi:10.24412/2227-7315-2021-2-145-152.

3. Гилева Н. С., Кайгородова О. В., Пинтий Н. И. Юридическая ошибка в уголовном праве Российской Федерации: понятие и последствия // Бизнес. Образование. Право. 2021. № 3 (56). С. 271–275. DOI: 10.25683/VOLBI.2021.56.368.

4. Дорогин Д. А. Разновидности юридической ошибки, исполнения уголовной ответственности // Lex Russica. 2019. № 8 (153). С 74-85. DOI: 10.17803/1729-5920.2019.153.8.074-085.

5. Едзати, Т. В. Фактическая ошибка в предмете и объекте посягательства / Т. В. Едзати, Р. Х. Бадоев // Научные труды студентов Горского Государственного аграрного университета «Студенческая наука - агропромышленному комплексу» : В 2-х частях. Том Выпуск 53, Часть 2. – Владикавказ : Горский государственный аграрный университет, 2016. – С. 332-334. – EDN WTJIMT.

6. Зайцева А.Ю. Юридическая и фактическая ошибки и их значение для квалификации преступления // Образование и право. 2013. № 9. С. 142-148.

7. Францева Ю.И. Уголовно-правовая ошибка: вопросы теории, законодательства и правоприменительной практики // Вестник Хабаровского государственного университета экономики и права. 2018. № 1. С. 119-122.

УДК 343.221

О. А. Кузнецова,
доктор юридических наук, доцент, главный научный сотрудник,
заведующий кафедрой,
Российский университет дружбы народов
имени Патриса Лумумбы,
М. М. Маджумаев,
кандидат юридических наук, ведущий научный сотрудник, старший преподаватель,
Российский университет дружбы народов
имени Патриса Лумумбы

Цифровой двойник (аватар) человека в метавселенной: альтер эго субъекта или средства преступления?

Аннотация. По мере того, как человеческие взаимодействия и взаимоотношения все больше перемещаются в цифровое (виртуальное) пространство, вопрос об особенностях применения материального уголовного права к деяниям, совершенным посредством цифрового аватара (или цифровыми аватарами), остается окончательно неурегулированным. Основной вопрос заключается в природе самого аватара: является ли он «альтер эго» субъекта, прямым продолжением личности, или же он всего лишь «инструмент», средство или агент, используемый для совершения преступления? Такое бинарное противопоставление, хотя и полезно в качестве отправной точки, чрезмерно упрощает сложную реальность и до конца не учитывает нюансы взаимоотношений между пользователем, его аватаром и лежащей в его основе технологией. В работе представлен модель атрибуции (приписания) ответственности за деяния цифрового двойника (аватара) в метавселенной.

Ключевые слова: метавселенная, метапреступление, цифровой двойник человека, аватар, субъект преступления, средство преступления, атрибуции (приписания) ответственности, доктрина снятия виртуальной вуали, ИИ-агент

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

O. A. Kuznetsova,
Doctor of Legal Sciences, Associate Professor, Chief Researcher,
Head of the Department,
Peoples' Friendship University of Russia named after Patrice Lumumba,
M. M. Madzhumayev,
Candidate of Legal Sciences, Leading Researcher, Senior Lecturer,
Peoples' Friendship University of Russia named after Patrice Lumumba

Human digital twin (avatar) in the metaverse: alter ego of the subject or instrument of crime?

Abstract. As human interactions and relationships increasingly extend into digital (virtual) space, the issue of how substantive criminal law applies to acts committed through a digital avatar (or by digital avatars) remains unresolved definitively. The essential question concerns the nature of the avatar itself: is it the subject's “alter ego”, a direct extension of their personality, or is it merely a “tool”, a means or agent used to commit a crime? Such a binary opposition, while useful as a starting point, oversimplifies a complex reality and does not fully take into account the nuances of the relationship between the user, their avatar, and the underlying technology. The paper presents a model of attribution (assignment) of responsibility for the actions of a digital twin (avatar) in the metaverse.

Keywords: metaverse, metacrime, human digital twin, avatar, perpetrator, instrument of crime, attribution of responsibility, doctrine of lifting the virtual veil, AI agent

Введение

Развитие метавселенной является показательным и беспрецедентным этапом в эволюции сети Интернет. Не ограничиваясь элементарными компьютерными играми или статичными веб-сайтами, метавселенная представляет собой постоянную, синхронную и иммерсивную виртуальную среду, в которой пользователи, представленные цифровыми аватарами, могут взаимодействовать друг с другом, с виртуальными объектами и с самим виртуальным миром [5]. Этот новый цифровой рубеж, направленный на слияние физической реальности с цифровым (виртуальным (VR), дополненным (AR), расширенным (XR)) существованием, порождает ряд характерных вызовов, требующих разработки новых подходов к регулированию и правил уголовно-правовой классификации. По мере того, как качественные различия между физическим «контактом» в реальном мире и виртуальным контактом в метавселенной постепенно стираются, становится все сложнее проводить грань между этими мирами. В условиях этой новой реальности возникают такие же новые виды вреда, квалификация которых по существующим правовым нормам требует переосмысления базовых институтов уголовного права.

В общем и целом, в «борьбе» с киберпреступностью, в частности с неправомерным доступом к компьютерной информации; созданием, использованием и распространением вредоносных компьютерных программ; нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также другими компьютерными преступлениями, достигнут определенный прогресс. Эти преступления в основном касаются манипулирования компьютерной информацией и системами. Вместе с тем проблема общественно опасных посягательств в метавселенной представляется гораздо более сложной, поскольку речь идет о новой форме преступности – «метапреступности», которая включает в себя такие посягательства, как преступления

против личности и в сфере экономики, совершаемые в виртуальном пространстве, но имеющие последствия в реальном мире. В частотности к метапреступлениям могут относиться преступления в сфере экономики, такие как хищение виртуальных активов (кража, мошенничество) [11. P. 181–214], легализация (отмывание) преступных доходов [7. P. 21–34] и, что еще более тревожно, преступления против личности, такие как виртуальные развратные действия и домогательства [6. P. 124–131]. Основная проблема заключается в том, что эти виртуальные действия, иногда не причиняя вреда в физическом мире «физическим» действием, могут активировать нервную систему и нанести эмоциональную и психологическую травму [3] жертвам с той же степенью воздействия, что и традиционные преступления.

Существующее законодательство с трудом (по понятным причинам) поспевает за этой технологической эволюцией. Традиционное уголовное право в значительной степени основано на физическом мире и ориентировано на деяния, которые требуют физических действий (бездействия) и физического присутствия, физических последствий, вытекающих из физических деяний. Как следствие, действующие нормативные правовые акты зачастую не применимы из-за несовместимости определенных характеристик виртуальных деяний с положениями уголовного права или являются недостаточными для «борьбы» с этими новыми виртуальными угрозами, поскольку требуют установления «физических элементов, а не виртуальных аналогий».

В этой связи закономерно возникает фундаментальный вопрос о возможности рассмотрения виртуального аватара как «альтер эго» субъекта преступления или же он является лишь средством совершения преступления. От ответа на этот вопрос зависит возможность инкриминирования (приписания) деяния субъекту, стоящему за аватаром. Как представляется, для решения данной проблемы необходим новый правовой подход. Именно в этом и заключается цель данной работы.

Основная часть

Цифровой двойник (аватар) человека в метавселенной как «альтер эго» субъекта

Представление о том, что аватар функционирует как альтер эго своего пользователя, основывается на экстраполяции подходов корпоративного права. Так, альтер эго, также известное как доктрина снятия корпоративной вуали [1. С. 224–231], позволяет отвергать юридическую фикцию корпоративной структуры и привлекать отдельных акционеров к личной ответственности за долги или правонарушения корпорации. Другими словами, согласно этой доктрине, при определенных условиях ответственность за обязательства юридического лица может быть возложена на его акционеров или других контролирующих лиц, независимо от положений закона об ограниченной ответственности акционеров и т. д. [1. С. 224–231]. Как правило, эта доктрина применяется в случаях, когда между юридическими лицами и физическими лицами существует единство интересов и собственности, а поддержание юридической фикции корпорации привело бы к нарушению законных интересов третьих лиц.

Представляется, что такой подход может стать концептуальной основой для преодоления виртуальной «вуали» аватара и привлечения к ответственности реального человека, стоящего за ним.

Для того чтобы подобная доктрина могла быть применена к пользователю и его аватару, между ними должна существовать очевидная связь. Такая связь может быть описана с помощью концепции «расширенного я» [4. P. 81–93]. Согласно этой концепции, личность человека выходит за пределы его физического тела и включает в себя его имущество и другие принадлежности [4. P. 81–93]. В этой связи, такая идея может быть распространена и на цифровые (виртуальные) пространства, где аватар будет рассматриваться как современная форма расширенной личности, глубоко интегрированной в идентичность пользователя.

Кроме того, связь между пользователем и аватаром (на анг. user-avatar bond), характеризует взаимоотношения, которые развиваются со временем в процессе взаимодействия пользователя со своим аватаром. Эта связь качественно отличается от других социальных отношений, поскольку пользователь в первую очередь передает свою волю через аватар, которым он манипулирует (управляет) различными способами. На прочность этой связи влияет уровень навыков пользователя. Для опытного пользователя аватар может настолько интегрироваться в его когнитивную систему, что функционирует как когнитивное расширение, позволяя пользователю воспринимать виртуальную среду и действовать в ней так, как если бы она была продолжением его собственного тела [8]. Это явление предполагает, что действия пользователя, выполняемые через строго контролируемый аватар, являются не просто использованием инструмента, а прямым результатом неразрывного психологического слияния, удовлетворяющего требованию единства интересов доктрины корпоративной вуали, что, в свою очередь, может претендовать на предоставление существенной основы для уголовной ответственности.

Цифровой двойник (аватар) человека в метавселенной как средство совершения преступления

В отличие от понимания аватара как альтер эго субъекта (его фактического продолжения), инструментальное понимание позволяет рассматривать аватар как простой инструмент, используемый для облегчения совершения преступления. Расценивая аватар как средство совершения преступления, его можно понимать как приспособление, с помощью которого была осуществлена объективная сторона преступления (совершено преступление). При этом аватар можно считать формой (или продуктом) программного обеспечения или телекоммуникационного устройства, а виртуальный мир отнести к компьютерной сети, посредством которой совершается преступление.

Наиболее очевидным доводом в пользу инструментальности аватара является техническая природа виртуальных пространств и различные степени контроля, осуществляемого пользователем. Даже если пользователь имеет сильную

психологическую связь со своим аватаром, фактическое преступное деяние может не быть результатом его непосредственной воли в реальном времени. Это особенно заметно, когда действия аватара являются полуавтономными, запрограммированными или полностью контролируемыми искусственным интеллектом. Агенты, управляемые искусственным интеллектом в их нынешнем виде, не обладают способностью проявлять человеческое намерение, т. е. осознавать общественную опасность своих действий (бездействия), предвидеть возможность или неизбежность наступления общественно опасных последствий и желать этих последствий (не желать их, а сознательно допускать их или относиться к ним безразлично). Как представляется, лицо, использующее такой ИИ-агент, который является своего рода источником повышенного риска, может быть привлечено к ответственности за небрежное использование ненадлежащим образом обученной программы искусственного интеллекта, которая причиняет вред, или за предсказуемые риски, создаваемые ее действиями.

Приведенная техническая реальность содержит принципиальный нюанс, который усложняет простое бинарное противопоставление «альтер эго» и «инструментальности» аватара.

Действия аватара не всегда являются результатом прямого управления в режиме реального времени со стороны пользователя с помощью контроллера, датчика взгляда или отслеживания рук (гаптика). Они также могут инициироваться пользователем, дающим высокоуровневую команду автономной системе, такой как скриптовое поведение или вовсе основанный на ИИ агент [2. P. 981–1004]. В этих случаях преступный умысел пользователя заключается не в том, чтобы совершить преступление непосредственно в этот момент, а в том, чтобы использовать инструмент для его совершения в дальнейшем (будущем). Таким образом, деяние, в смысле объективной стороны преступления, заключается не в движении аватара, а в действии пользователя по его использованию, программированию. По своей сути это соответствует принципу личной ответственности исполнителя (субъекта) за опасный агент.

Существование аватаров с искусственным интеллектом и скриптовым поведением требует более тонкого подхода, чем может быть обеспечен чистой моделью альтер эго или инструментальности. Пользователь, который дает указание автономному аватару совершить преступное деяние, не действует как альтер эго, а использует цифровой инструмент, аналогичный мобильному устройству или огнестрельному оружию, для совершения преступления. Такая точка зрения правильно фокусирует ответственность на сознательном выборе пользователя использовать преступный инструмент, независимо от кажущейся автономности аватара.

Модель атрибуции (приписания) ответственности за деяния аватара в метавселенной

Основная идея предлагаемой модели заключается в том, что уголовная ответственность за действия, совершаемые с использованием аватара (аватаром), не должна ограничиваться бинарным выбором, а представлять собой динамическую оценку, основанную на двух ключевых параметрах: степени контроля, осуществляемого пользователем, и связи между виртуальным действием и фактически причиненным ущербом.

Степень контроля пользователя над аватаром является основным фактором, определяющим применимый подход (альтер эго, инструментальный или иной). Может быть установлен ряд уровней контроля, начиная от прямых команд в режиме реального времени и заканчивая запуском полностью автономных скриптов, управляемых искусственным интеллектом.

Прямой контроль (высокая степень вовлеченности, исполнение) предполагает непосредственное управление аватаром пользователем в режиме реального времени. Например, когда пользователь использует контроллеры с шестью степенями свободы (6DoF), отслеживание движений рук или другие интуитивные методы ввода [9]. В этих сценариях аватар является прямым проводником воли пользователя. В этом случае наиболее применима подход аватар как альтер эго, поскольку пользователь и аватар имеют очевидное единство интересов. Преступный умысел пользователя может быть напрямую связан с действиями аватара, и это действие представляет собой физический акт управления аватаром с целью совершения преступного деяния, такого как виртуальное развратное действие, способное причинить реальную психологическую травму.

Полуавтономное управление (гибридное участие) применяется, когда пользователь инициирует заранее запрограммированное или полуавтономное действие, которое затем выполняется аватаром. Например, пользователь может дать команду высокого уровня автономному роботу или инициировать заранее запрограммированный скрипт [10. P. 237–250]. В этом случае аватар функционирует как инструмент (средство преступления), но намерение пользователя совершить преступление по-прежнему явно присутствует в акте развертывания. Это гибридная модель, в которой инструмент является признаком объективной стороны преступления, а высокая степень связи с намерением пользователя подразумевает наличие вины. Общественно опасным будут действия пользователя по созданию или развертыванию такого сценария.

Автономность, контролируемая искусственным интеллектом (ИИ-агент), предполагает, что пользователь использует полностью автономный аватар с искусственным интеллектом без прямого контроля в режиме реального времени. В этом случае аватар явно является средством совершения преступления (по крайней мере, при текущем уровне развития искусственного интеллекта (слабый ИИ)), и акцент смещается с действий аватара в метавселенной на действия пользователя по его использованию в объективной реальности. Действия ИИ-агента можно считать своего

рода источником повышенного риска. Пользователь может быть привлечен к ответственности за небрежное использование неправильно обученной программы искусственного интеллекта, которая причиняет вред, или за предсказуемые риски, создаваемые ее действиями. Действие будет представлять общественную опасность, если пользователь решит развернуть такое средство, и его вина (умысел) заключается в его осведомленности или безразличии в отношении потенциального вреда, который может причинить аватар.

Заключение

Ключевым вопросом при определении уголовной ответственности за преступления, совершенные с использованием цифровых двойников человека (аватаров) в метавселенной, является определение статуса этих виртуальных образов, а именно: являются ли они альтер эго пользователя или просто средством для совершения преступления? Такая постановка вопроса может быть чрезмерным упрощением сложной реальности метавселенных. Более надежным и научно обоснованным подходом было бы учет динамического характера отношений между аватаром и пользователем. В этой связи предлагаемая в настоящей работе модель основана на предположении, что ответственность должна определяться на основе двух основных параметров: степени контроля пользователя над аватаром и очевидной связи между виртуальным действием и фактическим ущербом.

В случае действий, совершаемых под прямым контролем пользователя в режиме реального времени, аватар функционирует как когнитивное продолжение, что оправдывает определение его как продолжения пользователя (экстраполируя доктрину снятия корпоративной вуали, в нашем случае, снятия виртуальной вуали). В таких случаях преступный умысел пользователя и само действие неразрывно связаны с действиями аватара. И наоборот, для действий, совершаемых полуавтономными или управляемыми искусственным интеллектом аватарами, доктрина инструментальности предоставляет более подходящую правовую основу. В этом случае вина лежит не на аватаре, а на сознательных действиях человека-пользователя, который использует ИИ-агента, что является источником повышенного риска совершения предсказуемого правонарушения.

В конечном итоге, представленная модель адаптирует фундаментальные принципы материального уголовного права к уникальному контексту виртуальных сред. Она предоставляет структурированную основу для определения ответственности и атрибуции действий цифрового двойника человека (аватара) в метавселенной, тем самым обеспечивая защиту от реального психологического, социального и финансового ущерба, который может быть причинен виртуальным неправомерным поведением.

Список литературы

1. Кондратьева К. С., Стерлигов И. А. Перспективы применения доктрины «снятия корпоративной вуали» при привлечении к субсидиарной ответственности контролирующих должника лиц в Российской Федерации: сравнительно-правовой подход // Вестник Томского государственного университета. 2021. №. 462. С. 224-231.

2. Acquaviva G. Crimes without Humanity? Artificial Intelligence, Meaningful Human Control, and International iminal Law // Journal of International Criminal Justice. 2023. Vol. 21. No. 5. pp. 981-1004. https://doi.org/10.1093/jicj/mqad024.

3. Bale A. S. et al. A comprehensive study on metaverse and its impacts on humans // Advances in Human-Computer Interaction. 2022. Vol. 2022. No. 1. P. 3247060. https://doi.org/10.1155/2022/3247060.

4. De Pisapia N. Understanding consciousness in the age of AI and XR: Altered states, emerging realities, and the digital self // Mind, Body, and Digital Brains. Cham : Springer Nature Switzerland, 2024. pp. 81-93. https://doi.org/10.1007/978-3-031-58363-6_6.

5. Han E. et al. People, places, and time: a large-scale, longitudinal study of transformed avatars and environmental context in group interaction in the metaverse // Journal of Computer-Mediated Communication. 2023. Vol. 28. No. 2. P. zmac031. https://doi.org/10.1093/jcmc/zmac031.

6. Melis G., Monaro M. Sexual Crimes in Metaverse: New Frontiers in Forensic Psychology and Legal Challenges // Journal of Metaverse. 2025. Vol. 5. No. 2. pp. 124-131. https://doi.org/10.57019/jmv.1658955.

7. Mooij A. Money laundering and financing of terrorism via the metaverse // Regulating the Metaverse Economy: How to Prevent Money Laundering and the Financing of Terrorism. Cham : Springer Nature Switzerland, 2023. pp. 21-34. https://doi.org/10.1007/978-3-031-46417-1_4.

8. Sah Y. J., Rheu M., Ratan R. Avatar-user bond as meta-cognitive experience: Explicating identification and embodiment as cognitive fluency // Frontiers in psychology. 2021. Vol. 12. P. 695358. https://doi.org/10.3389/fpsyg.2021.695358.

9. Uddin M. et al. Exploring the convergence of Metaverse, Blockchain, and AI: A comprehensive survey of enabling technologies, applications, challenges, and future directions // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2024. Vol. 14. No. 6. P. e1556. https://doi.org/10.1002/widm.1556.

10. Vaz J. C., Kosanovic N., Oh P. Art: Avatar robotics telepresence–the future of humanoid material handling loco-manipulation //Intelligent Service Robotics. 2024. Vol. 17. No. 2. pp. 237-250. https://doi.org/10.1007/s11370-023-00499-x.

11. Wu J. et al. What financial crimes are hidden in metaverse? Taxonomy and countermeasures // From Blockchain to Web3 & Metaverse. Singapore : Springer Nature Singapore, 2023. pp. 181-214. https://doi.org/10.1016/j.jeconc.2024.100118.

УДК 343.9:004.056

Д. А. Кунев,
кандидат юридических наук, доцент,
РАНХиГС,
заместитель начальника главного организационно-аналитического управления
Генеральной прокуратуры Российской Федерации –
начальник информационно-аналитического управления

Противодействие современным угрозам превентивными средствами: российский опыт

Аннотация. Статья посвящена анализу российского опыта противодействия киберпреступности в условиях стремительного развития информационных технологий и цифровизации экономики. Рассматриваются нормативно-правовые и организационные основы борьбы с преступлениями в цифровой среде, практика использования антифрод-систем и блокчейн-аналитики, а также внедрение технологий искусственного интеллекта в деятельность прокуратуры. Особое внимание уделяется вопросам противодействия преступлениям с использованием криптовалют и иных виртуальных активов. Делается вывод о необходимости комплексного подхода, включающего профилактику, правовое регулирование и применение инновационных технологий в правоохранительной деятельности.

Ключевые слова: киберпреступность, цифровая среда, прокуратура, антифрод-системы, криптовалюта, виртуальные активы, искусственный интеллект, DE-FI-преступность

D. A. Kunev,
Candidate of Law, Deputy Head of the Main Organizational and Analytical Directorate – Head of the Information and Analytical Directorate, Office of the Prosecutor General of the Russian Federation

Countering modern threats with preventive means: russian experience

Abstract. The article analyzes the Russian experience of countering cybercrime in the context of rapid development of information technologies and digitalization of the economy. The article examines the regulatory and organizational framework for combating crimes in the digital environment, the practice of using antifraud systems and blockchain analytics, as well as the introduction of artificial intelligence technologies in the activities of the prosecutor's office. Particular attention is paid to the issues of countering crimes using cryptocurrencies and other virtual assets. A conclusion is made about the need for an

integrated approach, including prevention, legal regulation and the use of innovative technologies in law enforcement.

Keywords: cybercrime, digital environment, prosecutor's office, antifraud systems, cryptocurrency, virtual assets, artificial intelligence, DE-FI crime

Введение

Стремительное развитие информационных технологий, цифровизация государственного управления и экономики сопровождаются ростом киберугроз, масштабы и трансграничный характер которых ставят перед государством и правоохранительными органами принципиально новые задачи. В России четверть всех регистрируемых преступлений совершается с использованием современных цифровых технологий, противодействие киберпреступности стало одним из приоритетных направлений государственной политики [3].

Цель настоящей статьи – обобщить ключевые направления противодействия киберпреступности в Российской Федерации, опираясь на опыт Генеральной прокуратуры Российской Федерации и практику применения законодательства, а также обозначить перспективные направления профилактики и реагирования на угрозы в цифровой среде.

Основная часть

Развитие цифровой экономики в России сопровождается формированием комплексной нормативно-правовой базы, обеспечивающей регулирование цифровой среды. Так, продолжаются отдельные мероприятия национального проекта «Цифровая экономика», в рамках которого активно развиваются информационная инфраструктура и новейшие технологии, укрепляется кадровый потенциал, включая повышение квалификации сотрудников правоохранительных органов, а также внедрение искусственного интеллекта в правоохранительную деятельность [2].

В последние годы приняты многочисленные законодательные акты, направленные на предотвращение мошенничества в сети, защиту персональных данных, регулирование оборота виртуальных активов, а также совершенствование инструментов расследования киберпреступлений.

Генеральная прокуратура Российской Федерации как координатор борьбы с преступностью в стране уделяет приоритетное внимание вопросам кибербезопасности, вырабатывает методические подходы и инициирует законодательные поправки, обеспечивающие возможность эффективного противодействия новым формам преступности.

Одним из наиболее распространенных видов преступлений в цифровой среде является мошенничество, включая телефонные и интернет-схемы.

Эффективным средством его предупреждения стало внедрение антифрод-систем, позволяющих блокировать звонки от мошенников, выявлять подозрительные операции и предотвращать хищения денежных средств.

Наряду с этим, прокуратура добилась привлечения операторов связи к ответственности за несоблюдение обязанностей по блокировке мошеннических звонков. В результате количество предотвращенных противоправных транзакций исчисляется миллионами.

Генеральная прокуратура на системной основе инициирует поправки в законодательство, которые блокируют и другие схемы виртуальных мошенников. Например, в 2024 году усовершенствованы механизмы борьбы с хищением денег с банковских счетов граждан, возмещения ущерба и блокирования средств мошенников. По результатах проверок и расследований, проведенных в связи с цифровыми преступлениями, в законодательство внесены нормы, обязывающие банки отказывать в проведении операций по счетам, если в базе данных Банка России есть сведения об их связях с лицами, подозреваемыми в мошенничестве. Такие транзакции проверяются одновременно как банком плательщика, так и банком получателя.

Кроме того, уголовное и уголовно-процессуальное законодательства дополнены десятками поправок: от ответственности за администрирование «сим-банков» и нелегальных баз данных до возможности замораживать подозрительные банковские операции.

Особое значение приобретает борьба с преступлениями, связанными с использованием криптоактивов. Российская правоохранительная практика уже включает примеры ареста виртуальных активов на международных криптобиржах, что стало возможным благодаря взаимодействию прокуратуры и следственных органов с операторами криптовалютных платформ.

Применение отечественного программного обеспечения на основе технологий блокчейна позволило повысить эффективность расследований, выявлять цепочки незаконных транзакций и участников преступных схем. Отдельного внимания заслуживает формирование практики по противодействию DE-FI–преступности», включающей использование невзаимозаменяемых токенов (NFT), виртуальных предметов в онлайн-играх и иных децентрализованных активов [4].

Современные вызовы обусловили внедрение технологий искусственного интеллекта в деятельность прокуратуры. К числу приоритетных направлений относятся машинная аналитика, интеллектуальное прогнозирование, совершенствование обработки обращений граждан. Нейросетевые технологии позволяют автоматизировать поиск цифровых следов, выявлять аномалии в финансовых транзакциях и моделировать возможные сценарии развития преступных практик. При этом центральной фигурой в принятии решений остается человек, а искусственный интеллект рассматривается как вспомогательный инструмент, повышающий эффективность и скорость аналитической работы [1].

Опыт Российской Федерации демонстрирует, что противодействие киберугрозам требует комплексного подхода, включающего:

– профилактику преступлений и правовое просвещение населения;

– использование современных технологий (антифрод-систем, блокчейн-аналитики, искусственного интеллекта);

– совершенствование законодательства с учетом динамики цифровой среды;

– консолидацию усилий правоохранительных органов под координацией прокуратуры.

Заключение. Российская модель противодействия киберпреступности сочетает правовые, организационные и технологические меры, ориентированные на опережающее реагирование и устранение причин киберугроз. При этом понятие киберпреступности не стоит путать с другими достаточно близкими категориями [5. С. 119].

Список литературы

1. Кунев Д.А., Симонов А.А. Развитие технологий искусственного интеллекта как перспективное направление цифровой трансформации органов прокуратуры // Вестник Университета прокуратуры Российской Федерации. 2024. № 3 (101). С. 27-33.

2. Паспорт национального проекта «Цифровая экономика Российской Федерации». Утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам 24.12.2018 // [Электронный ресурс]. URL: СПС «КонсультантПлюс» (дата обращения: 05.09.2025).

3. Статистические данные МВД России о состоянии преступности в 2025 году // [Электронный ресурс]. URL: https://мвд.рф (дата обращения: 05.09.2025).

4. Цифровое право: учебник / под общ. ред. Э.Л. Сидоренко. М.: Проспект. 2024. С. 600-608.

5. Шутова А. А. Соотношение информационной, кибер- и цифровой безопасности // Наука, общество, инновации: актуальные вопросы современных исследований : Сборник статей VIII Международной научно-практической конференции, Пенза, 10 сентября 2025 года. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2025. С. 119-122. EDN PNOEIH.

УДК 343.7

М. В. Кушнир,
помощник депутата Государственной Думы М.В. Бутиной
по работе в Государственной Думе

Применение цифровых технологий в Уголовном законодательстве Российской Федерации

Аннотация. Настоящая статья посвящена анализу современного состояния и перспектив применения цифровых технологий в сфере уголовного законодательства Российской Федерации. В условиях стремительного развития информационного общества и цифровизации государственного управления особую актуальность приобретает вопрос интеграции инновационных технологических решений в правоприменительную практику и законотворческий процесс. Автор исследует основные направления внедрения цифровых технологий в уголовно-правовую сферу, включая электронное досудебное производство, цифровые доказательства, системы искусственного интеллекта для анализа правонарушений и автоматизированные системы принятия процессуальных решений. Особое внимание уделяется анализу нормативно-правового регулирования данных процессов и выявлению проблемных аспектов цифровой трансформации уголовного права. Исследование базируется на анализе действующего российского законодательства, судебной практики и научных разработок в области цифровизации правовой системы. В результате формулируются выводы о необходимости системного подхода к цифровой модернизации уголовного законодательства при обеспечении баланса между технологической эффективностью и соблюдением конституционных прав граждан.

Ключевые слова: цифровые технологии, уголовное законодательство, электронное правосудие, цифровые доказательства, искусственный интеллект, правоприменение, цифровизация, информационные системы, автоматизация, правовое регулирование

M. V. Kushnir,
Assistant to the deputy of the State Duma M.V. Butina
for work in the State Duma

Application of digital technologies in Criminal Law of the Russian Federation

Abstract. This article is devoted to the analysis of the current state and prospects of the application of digital technologies in the field of criminal legislation of the Russian Federation. In the context of the rapid development of the information society and the digitalization of public administration, the issue of integrating innovative technological solutions into law enforcement practice and the legislative process is becoming particularly relevant. The author explores the main directions of the introduction of digital technologies

in the criminal law sphere, including electronic pre-trial proceedings, digital evidence, artificial intelligence systems for the analysis of offenses and automated systems for making procedural decisions. Special attention is paid to the analysis of the legal regulation of these processes and the identification of problematic aspects of the digital transformation of criminal law. The research is based on an analysis of current Russian legislation, judicial practice and scientific developments in the field of digitalization of the legal system. As a result, conclusions are drawn about the need for a systematic approach to the digital modernization of criminal legislation while ensuring a balance between technological efficiency and respect for the constitutional rights of citizens.

Keywords: digital technologies, criminal law, electronic justice, digital evidence, artificial intelligence, law enforcement, digitalization, information systems, automation, legal regulation

Введение

Современный этап развития российского государства характеризуется масштабной цифровой трансформацией всех сфер общественной жизни, включая правовую систему [1]. Национальная программа «Цифровая экономика Российской Федерации» определила стратегические приоритеты цифровизации государственного управления, что непосредственно затрагивает сферу уголовного законодательства [2] и правоприменительной практики [3, 4].

Цифровые технологии в уголовно-правовой сфере представляют собой комплекс инновационных решений, направленных на повышение эффективности правоохранительной деятельности, оптимизацию судебных процедур и обеспечение более точного и справедливого применения уголовного закона. Вместе с тем внедрение цифровых технологий в столь консервативную и социально значимую область права требует тщательного научного анализа и взвешенного нормативного регулирования.

Основная часть

Процесс цифровизации российского уголовного законодательства осуществляется по нескольким ключевым направлениям [5]. Первоначально цифровые технологии проникли в сферу документооборота и делопроизводства правоохранительных органов. Создание единых информационных систем, таких как ГАС «Правосудие» и ФГИС «Досудебное производство», заложило основу для комплексной автоматизации уголовного процесса.

Особое значение приобретает развитие института электронного уголовного дела, который позволяет существенно ускорить процессуальные действия и повысить качество их документирования. Федеральный закон от 23.06.2016 № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» создал правовую основу для широкого использования электронных документов в судебной деятельности.

Значительным шагом вперед стало внедрение систем видеоконференцсвязи в судебных заседаниях, что особенно актуализировалось в период пандемии COVID-19. Данная технология не только обеспечила непрерывность правосудия в условиях ограничительных мер, но и продемонстрировала потенциал цифровых решений для повышения доступности правосудия.

Одним из наиболее динамично развивающихся направлений применения цифровых технологий в уголовном праве является институт цифровых доказательств. Современные преступления все чаще совершаются с использованием информационно-телекоммуникационных технологий, что порождает новые виды доказательств – электронные следы, цифровые отпечатки, метаданные файлов и системные логи.

Российский законодатель постепенно адаптирует процессуальное законодательство к реалиям цифрового общества. Статья 84 УПК РФ была дополнена положениями об электронных документах как разновидности документов-доказательств. Однако правовое регулирование в данной сфере остается фрагментарным и требует системного подхода к определению процедур собирания, проверки и оценки цифровых доказательств.

Криминалистическая экспертиза компьютерной информации становится неотъемлемой частью расследования многих категорий уголовных дел. Развитие методик цифровой криминалистики позволяет извлекать доказательственную информацию из мобильных устройств, облачных хранилищ, систем видеонаблюдения и иных источников цифровых данных.

Перспективным направлением цифровизации уголовного права является внедрение технологий искусственного интеллекта. Системы машинного обучения и нейронные сети могут существенно повысить эффективность аналитической работы правоохранительных органов, обеспечить прогнозирование криминальных угроз и оптимизировать распределение ресурсов для борьбы с преступностью.

Алгоритмы искусственного интеллекта находят применение в анализе больших массивов данных о преступности, выявлении латентных связей между участниками преступных групп, прогнозировании рецидива и оценке рисков при принятии процессуальных решений. В некоторых зарубежных юрисдикциях системы искусственного интеллекта уже используются для помощи судьям в определении мер пресечения и назначении наказания.

Вместе с тем применение искусственного интеллекта в уголовном праве порождает серьезные этические и правовые дилеммы. Алгоритмическое принятие решений может содержать скрытые предрассудки и дискриминационные элементы, что противоречит принципам равенства перед законом и презумпции невиновности. Необходимо обеспечить прозрачность алгоритмов и возможность их судебного контроля.

Цифровая трансформация уголовного права сопряжена с рядом системных проблем и вызовов. Прежде всего, это вопросы кибербезопасности и защиты

персональных данных участников уголовного процесса. Концентрация чувствительной информации в цифровых системах создает новые риски утечек и несанкционированного доступа к конфиденциальным данным.

Существенной проблемой является цифровое неравенство, которое может ограничить доступ отдельных категорий граждан к правосудию. Необходимо обеспечить альтернативные каналы взаимодействия с правоохранительными органами и судами для лиц, не владеющих цифровыми технологиями.

Особую озабоченность вызывает потенциальная дегуманизация правосудия в результате чрезмерной автоматизации процессуальных решений. Уголовное право затрагивает фундаментальные права человека, и любые технологические решения должны сохранять человеческий контроль над принятием ключевых решений.

Дальнейшее развитие цифровых технологий в уголовном праве должно осуществляться на основе системного подхода и с учетом международного опыта. Необходимо совершенствование нормативно-правовой базы, создание единых стандартов цифрового взаимодействия в правоохранительной сфере и развитие компетенций сотрудников правоохранительных органов в области цифровых технологий.

Перспективными направлениями являются развитие блокчейн-технологий для обеспечения неизменности доказательств, внедрение биометрической идентификации участников процесса, создание интеллектуальных систем правового анализа и автоматизированного мониторинга исполнения судебных решений.

Заключение

Применение цифровых технологий в уголовном законодательстве Российской Федерации представляет собой объективную необходимость, обусловленную развитием информационного общества и потребностями модернизации правоохранительной системы. Вместе с тем, цифровизация уголовного права требует взвешенного подхода, обеспечивающего баланс между технологической эффективностью и соблюдением конституционных принципов правосудия.

Успешная реализация потенциала цифровых технологий в уголовно-правовой сфере возможна лишь при условии комплексного реформирования нормативно-правовой базы, развития профессиональных компетенций правоприменителей и обеспечения надежной защиты прав граждан в цифровой среде. Дальнейшие исследования в данной области должны сосредоточиться на разработке эффективных механизмов правового регулирования цифровых процессов и этических стандартов применения инновационных технологий в правосудии.

Список литературы

1. Бородинова, Т. Г. Цифровые технологии в уголовном судопроизводстве России: пределы и проблемы внедрения / Т. Г. Бородинова // Правосудие. – 2022. – Т. 4, № 1. – С. 71-86. – DOI 10.37399/2686-9241.2022.1.71-86. – EDN DVLLBY.

2. Долгов, А. М. Правовые основы применения цифровых технологий в уголовном процессе России / А. М. Долгов // Теория и практика общественного развития. – 2020. – № 12(154). – С. 72-74. – DOI 10.24158/tipor.2020.12.13. – EDN KLCGGY.

3. Марковичева, Е. В. Цифровая трансформация российского уголовного судопроизводства / Е. В. Марковичева // Правосудие. – 2020. – Т. 2, № 3. – С. 86-99. – DOI 10.37399/2686-9241.2020.3.86-99. – EDN RLPPEO.

4. Бегишев, И. Р. Правовое регулирование беспилотных транспортных средств / И. Р. Бегишев // Транспортное право. – 2021. – № 3. – С. 7-10. – DOI 10.18572/1812-3937-2021-3-7-10. – EDN BFFKKJ.

5. Меретуков, Г. М. Актуальные вопросы цифровизации уголовного судопроизводства: взгляд в будущее / Г. М. Меретуков, С. И. Грицаев, В. В. Помазанов // Правоприменение. – 2022. – Т. 6, № 3. – С. 172-185. – DOI 10.52468/2542-1514.2022.6(3).172-185. – EDN GVZMZH.

УДК 343.140.02

Э. Ю. Латыпова,
кандидат юридических наук, доцент,
заведующий кафедрой,
Казанский инновационный университет
имени В. Г. Тимирясова,
Э. Е. Азаров,
студент,
Казанский инновационный университет
имени В. Г. Тимирясова

Риски «цифровой стигматизации»: учет цифрового следа личности при назначении наказания

Аннотация. Рассмотрены особенности использования цифрового следа личности при назначении наказания в уголовном процессе. Акцентируется внимание на рисках формирования негативного образа подсудимого на основании неполных или искаженных цифровых данных, обозначая данное явление термином «цифровая стигматизация». Приводится перечень основных угроз, в числе которых нарушение презумпции невиновности, недостоверность и контекстуальные искажения цифровой информации, предвзятость и эффект «вечной памяти». В заключении сформулированы предложения по минимизации рисков цифровой стигматизации, включая нормативное закрепление допустимости цифровых данных, принцип релевантности и обязательность экспертной проверки их достоверности.

Ключевые слова: цифровая стигматизация, цифровой след личности, назначение наказания, цифровизация, цифровое досье, презумпция невиновности, предсказательная криминология

E. YU. Latypova,
Candidate of Law, Associate Professor
Kazan Innovative University
named after V.G. Timiryasov,
E. E. Azarov,
student
Kazan Innovative University
named after V.G. Timiryasov

Risks of "digital stigmatization": taking into account the digital footprint of a person when imposing punishment

Abstract. The features of the use of a digital personality trace in the appointment of punishment in the criminal process are considered. Attention is focused on the risks

of forming a negative image of the defendant based on incomplete or distorted digital data, referring to this phenomenon by the term "digital stigmatization". The list of the main threats is given, including violation of the presumption of innocence, unreliability and contextual distortion of digital information, bias and the "eternal memory" effect. In conclusion, proposals are formulated to minimize the risks of digital stigmatization, including the normative consolidation of the permissibility of digital data, the principle of relevance and the obligation of expert verification of their reliability.

Keywords: digital stigmatization, digital personality trace, sentencing, digitalization, digital dossier, presumption of innocence, predictive criminology

Введение. Столь быстрое, а равно глобальное развитие цифровых технологий оказало фундаментальное влияние на все сферы общественной жизни, включая такую специфическую, как уголовное судопроизводство. Наряду с привычными источниками, посредством которых осуществляется сбор необходимых данных о личности подсудимого или обвиняемого, в настоящее время практика стала перенимать новые формы, отражающие поведение лиц в цифровой среде. Речь идет о так называемом цифровом следе личности или цифровом облике, под которым мы понимаем совокупность данных, формируемых в результате активности индивида в информационно-телекоммуникационной среде, в том числе в сети «Интернет», социальных сетях, мессенджерах, а также посредством использования устройств для передачи, хранения и обработки информации.

На наш взгляд, включение таких сведений в характеристику личности обвиняемого при назначении наказания вызывает ряд социально значимых рисков. Основным из них является формирование негативного образа лица на основе неполных, искаженных или контекстуально неверно интерпретированных цифровых данных. Данное явление можно обозначить термином «цифровая стигматизация», отражающим опасность закрепления за личностью устойчивого социального ярлыка, негативно влияющего на конечное судебное решение.

Основная часть. На протяжении десятилетий уголовное судопроизводство уделяет значительное внимание характеристике личности подсудимого. В соответствии со статьей 60 УК РФ, при назначении наказания учитываются обстоятельства, характеризующие личность виновного, в том числе обстоятельства, смягчающие и отягчающие наказание, а также влияние назначенного наказания на исправление осужденного и на условия жизни его семьи.

Вместе с фундаментальными устоями правосудия, а также основами оперативной работы, цифровизация расширяет этот спектр, включая в него: открытые данные, выраженные посредством публикации в социальных сетях, оставленные комментарии, опубликованные на общее обозрение фотографии, а равно публичные высказывания. При этом мы рассматриваем и противоположную группу данных, ранее отмеченных, а именно закрытые данные, включающие информацию о транзакциях,

геолокации, личной переписке, иных сведений, составляющих личную или семейную тайну [5. С. 37] истребованных или выявленных в ходе проведения следственных действий.

Таким образом, как мы являемся свидетелями того, как цифровой след или облик становится новой составляющей так называемого «цифрового досье личности» [7], способного оказать влияние на оценку подсудимого судом.

Цифровые данные могут использоваться как доказательства негативных факторов, изобличающих личность, что противоречит принципу презумпции невиновности. Например, публикации в социальных сетях способны трактоваться как признаки криминальной идеологии, хотя не имеют прямого отношения к рассматриваемому преступлению. Цифровая информация подвержена манипуляциям из вне. Запечатленные посредством функции «скриншот» данные могут быть сфальсифицированы в интересах третьих лиц, записи вырваны из контекста, а устаревшие сведения восприниматься как актуальные [1. С. 13]. Вместе с тем, отметим и возрастающие случаи использования искусственного интеллекта для предания реальности словам и идеям, а также противоправным действиям посредством технологии «дипфейк». Именно поэтому сейчас в социальных сетях массово стали распространяться различного рода ложные сведения [2. С. 109], что ранее, даже десять лет назад, представить было достаточно сложно [6. С. 36]. Это, в свою очередь, можно рассматривать как фактор, снижающий достоверность цифровой характеристики индивида. Даже удаленные публикации или иные данные продолжают существовать в кэшах, архивах и базах данных. Это создает эффект «неизбывного прошлого», когда цифровые следы преследуют человека на протяжении всей жизни, и даже после ее биологического завершения, тем самым формируя его негативный образ. Внедрение предсказательной криминологии и алгоритмических систем в правосудие может привести к тому, что цифровой профиль станет основой для прогнозирования будущих правонарушений.

Для снижения угрозы цифровой стигматизации необходимо внедрение комплексных мер, таких, как нормативное закрепление рамок допустимости изучения и приобщения цифровых данных при назначении наказания и их объема. Необходимо использовать принцип релевантности применительно к пониманию учета только тех сведений, которые имеют прямое отношение к рассматриваемому уголовному делу. Также нужно обеспечение достоверности, путем введения обязательной экспертной проверки цифровых доказательств, как самостоятельного и взаимосвязанного этапа такой проверки. Аналогичные требования можно распространить и на уголовно-процессуальные действия с участием иностранных граждан [4. С. 370].

Необходимо не допускать распространения цифровой информации, полученной в результате следственных или судебных действий [3. С. 40], с целью предотвращения утечки такой информации или использования иными лицами в преступных целях.

Заключение. Цифровизация уголовного судопроизводства открывает новые возможности, но одновременно привносит значительные риски. Учет цифрового следа личности при назначении наказания способен как повысить объективность судебной оценки, так и привести к цифровой стигматизации, что послужит формированию негативного образа подсудимого на основании искаженных либо нерелевантных данных. Для минимизации этих рисков необходимо разработать комплексное правовое регулирование, включающее закрепление принципа релевантности цифровых сведений и обязательность проверки их достоверности. Перспективным направлением представляется разработка междисциплинарного стандарта оценки цифровых данных в уголовно-правовой сфере, что позволит обеспечить баланс между интересами правосудия и защитой прав личности в условиях цифровизации.

Список литературы

1. Блохина А. А. Проблема раскрываемости информационных преступлений в сфере завладения персональными данными физического лица / В сборнике: Наука. Образование. Инновации: современное состояние актуальных проблем. Сборник научных трудов по материалам I Международной научно-практической конференции. Анапа: Изд-во ООО «Научно-исследовательский центр экономических и социальных процессов» в Южном Федеральном округе, 2022. С. 6-12.

2. Гильманов Р. Э., Азаров Э. Е. СМИ как инструмент влияния на общественное мнение и ответственность за его использование / В сборнике: Цифровые технологии и право: Сборник научных трудов III Международной научно-практической конференции. В 6-ти томах. Казань, 20 сентября 2024 года / под ред. И.Р. Бегишева [и др.]. Том 3. Казань: Изд-во «Познание» Казанского инновационного ун-та, 2024. С. 107-111.

3. Гильманов Э.М., Гильманов Р.Э., Азаров Э.Е. Ответственность за раскрытие посредством сети Интернет данных, ставших известными в ходе проведения следственных действий / В сборнике: Цифровые технологии и право: Сборник научных трудов III Международной научно-практической конференции. В 6-ти томах. Казань, 20 сентября 2024 года / под ред. И.Р. Бегишева [и др.]. Том 3. Казань: Изд-во «Познание» Казанского инновационного ун-та, 2024. С. 107-111.

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

5. Латыпова Э.Ю. Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Oeconomia et Jus. 2019. № 2. С. 35–45.

6. Латыпова Э.Ю., Гильманов Р.Э. Уголовно-правовая ответственность за распространение фейков в социальных сетях // В сборнике: Цифровые технологии

и право: Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года / под ред. И.Р. Бегишева [и др.]. Том 5. Казань: Изд-во «Познание» Казанского инновационного ун-та, 2023. С. 36-39.

7. Begishev I., Shutova A., Allonazarov O., Denisovich V., Latypova E. Technological Transformation of Professional Communication in Society 5.0 // В сборнике: 2025 Communication Strategies in Digital Society Seminar (ComSDS). IEEE, 2025. С. 219-223.

УДК 343.9

Т. М. Лопатина,
доктор юридических наук, профессор,
заведующий кафедры,
Смоленский государственный университет,
профессор кафедры,
Международный юридический институт

Преступность в цифре: генезис, типология и вызовы современности

Аннотация. Статья посвящена комплексному анализу феномена цифровой преступности как качественно нового этапа эволюции криминальной деятельности. Рассматриваются предпосылки ее возникновения, ключевые характеристики (трансграничность, анонимность, технологичность, латентность), а также динамика развития. Особое внимание уделяется эволюции тактик злоумышленников, экономическим и социальным последствиям цифровой преступности, а также системным вызовам для правоохранительных органов и общества в целом. Делается вывод о необходимости формирования адаптивных, технологичных и международно-согласованных стратегий противодействия.

Ключевые слова: цифровая преступность, киберпреступность, киберугрозы, компьютерные преступления, криптопреступность, фишинг, вредоносное ПО, программы-вымогатели, DDoS-атаки, Darknet, цифровая криминалистика, кибербезопасность

T. M. Lopatina,
Doctor of Law, Head of the Department,
Smolensk State University,
Professor, International Law Institute

Digital crime: genesis, typology, and challenges of the present

Abstract. The article is devoted to a comprehensive analysis of the phenomenon of digital crime as a qualitatively new stage in the evolution of criminal activity. It examines the prerequisites for its emergence, key characteristics (cross-border, anonymous, technological, and latent), as well as the dynamics of its development. Special attention is paid to the evolution of malicious actors' tactics, the economic and social consequences of digital crime, and the systemic challenges it poses for law enforcement agencies and society as a whole. The article concludes that it is necessary to develop adaptive, technological, and internationally coordinated strategies for countering digital crime.

Keywords: digital crime, cybercrime, cyber threats, computer crimes, cryptocryminality, phishing, malware, ransomware, DDoS attacks, Darknet, digital forensics, cybersecurity

Введение. Цифровые технологии, быстро развиваясь, формируют цифровое государство, которое характеризуется существенными положительными и отрицательными изменениями, а также имеет в себе достаточно большой потенциал криминологических рисков. Более того, мы строим цифровую экономику, трансформируемся в цифровое пространство, но при этом не имеем структурированного подхода на проблему преступности цифрового мира. Цифровая революция кардинально трансформировала не только легальные аспекты жизни общества, но и криминальную среду. Мы просто констатируем факт расширения масштабов цифровой преступности, которая представляет собой не просто новое криминологическое явление, а важную государственную и общественную проблему, обусловленную доступностью способа совершения преступлений человеком, на примитивном уровне разбирающемся в программировании.

Возник новый вид преступности – «преступность в цифре», как широкий спектр общественно опасных деяний, совершаемых с использованием или в отношении информационно-телекоммуникационных систем и сетей, либо преступлений традиционного характера, перенесенных в цифровую среду и приобретших новые масштабы и формы. Эта преступность характеризуется беспрецедентной скоростью эволюции, глобальным охватом и значительным экономическим ущербом, становясь одним из ключевых вызовов национальной и международной безопасности XXI века.

Основная часть. «Понятие «цифровая преступность» в настоящее время на законодательном уровне отсутствует в виду присутствия так называемой юрисдикционной дилеммы. Есть опыт в исследовании и определении понятия киберпреступности, но он не дает полной картины и определения тех преступлений, которые совершаются в сфере цифровых технологий или с их использованием» [4. С. 12].

В одной из первых монографий, посвященных анализу компьютерных преступлений, последние вообще подразделялись на две группы: «преступления, связанные с вмешательством в работу компьютеров и преступления, использующие компьютеры как необходимые технические средства» [4. С. 11, 7. С. 75].

При этом следует обратить внимание, что «в материалах одиннадцатого Конгресса ООН речь идет уже не о киберпреступности, а преступлениях с использованием современных информационных и цифровых технологий. Но понятие «цифровая преступность» практически не используется» [2. С. 216–218].

В настоящее время в уголовном законе присутствует квалифицирующий признак «с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)», который предусмотрен в 20-ти нормах Особенной части УК РФ (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110^1, ч. 2 ст. 110^2, ч. 2 ст. 128^1, п. «б» ч. 3 ст. 133, ч. 3 ст. 137, п. «в» ч. 2 ст. 151^2, ч. 1 ст. 159^6, ч. 1 ст. 171^2 и др.).

Следовательно, преступления с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)» – это как компьютерные

преступления, так и общеуголовные компьютеризированные преступления, посягающие на традиционно охраняемые уголовным законом общественные отношения. Более того, ряд авторов относит их к высокотехнологичным [3. С. 240–243, 8. С. 15, 9. С. 25–32]. По их мнению, ключевыми понятиями является именно использование информационно-телекоммуникационных технологий.

С позиции уголовного права возможно это и так, но с распространением информационно-технологического способа совершения преступлений и с развитием цифровых технологий, на наш взгляд, необходимо рассматривать данную проблему шире.

В сложившейся криминогенной обстановке следует не только соотносить понятия компьютерная преступность и преступления, совершаемые с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)», но и понятия «цифровая преступность». Цифровые технологии используются в вычислительной электронике, а значит как в компьютерах, так и в информационно-телекоммуникационных сетях, включая Интернет. Они применяются в средствах сбора, хранения, анализа и обмена информации (игровые автоматы, робототехника, различные измерительные приборы, кино, телевидение и др.). Более того, распространение вредоносных программ может осуществляться через компьютер, Интернет и через технологии MMS, Bluetooth и другие цифровые программы [4. С. 121].

Понятия «цифровая преступность», «цифровые преступления», «преступления, совершаемые в сфере цифровых технологий» и «преступность в сфере цифровых технологий» в настоящее время находятся на стадии доктринальных дискуссий.

Цифровая преступность является закономерным следствием:

– всеобщей цифровизации: перенос в онлайн бизнеса, финансов, коммуникаций, государственных услуг создал новые цели и возможности для преступников;

– экономической мотивации, поскольку имеет потенциал для получения огромных незаконных доходов при относительно низких рисках обнаружения и привлечения к уголовной ответственности. Годовой глобальный ущерб от киберпреступности измеряется триллионами долларов США (по данным различных отчетов IBM, McAfee, Cybersecurity Ventures);

– трансграничности интернета, который стирает физические границы государств, они не являются препятствием для кибератак, что создает проблемы с юрисдикцией и задержанием преступников;

– доступности технологий в виде хакерских инструментов (вредоносное ПО, инструменты для DDoS), криптографии, анонимизирующих сервисов (Tor, VPN) и сервисов «преступление как услуга» (Crime-as-a-Service, CaaS).

Классификация современной цифровой преступности может быть проведена по объекту посягательства и способу совершения.

С учетом объекта посягательства к цифровым преступлениям относятся:

– классические компьютерные преступления, посягающие на безопасность информации и систем: ст. ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», а также компьютерный саботаж (DDoS-атаки, вывод систем из строя);

– преступления против собственности, совершаемые с использованием ИКТ: кибермошенничество (фишинг, вишинг, смишинг, CEO-мошенничество, мошенничество с платежами, кардинг); вымогательство (программы-вымогатели «Ransomware», блокирующие доступ к данным или системам; шантаж с угрозой обнародования компрометирующей информации (doxing), полученной путем взлома; кража криптовалют (взломы криптобирж и кошельков, криптоджекинг (несанкционированное использование вычислительных мощностей для майнинга);

– преступления против конституционных прав и свобод человека и гражданина: нарушение неприкосновенности частной жизни (несанкционированный сбор и распространение персональных данных, шпионское ПО); клевета и оскорбление в соцсетях (травля, кибербуллинг); неправомерный доступ к переписке;

– преступления против общественной безопасности и государственной власти: кибертерроризм (атаки на критическую информационную инфраструктуру (КИИ): энергетика, транспорт, связь, финансы); распространение экстремистских материалов, вербовка в террористические организации; государственный кибершпионаж; манипулирование информацией (дезинформация, фейк-ньюс) с целью дестабилизации обстановки в государстве и обществе;

– традиционные общеуголовные преступления, перенесенные в цифровую среду: незаконный оборот наркотиков, оружия, поддельных документов (через Darknet-маркетплейсы); организация проституции; отмывание денег (криптомиксеры, фиктивные онлайн-компании).

С учетом способа совершения к цифровым преступлениям могут быть отнесены:

– преступления против жизни и здоровья (ст. 110–110^2, 119 УК РФ),

– преступления против свободы, чести и достоинства (ст. 128^1 УК РФ),

– преступления против конституционных прав и свобод человека и гражданина (ст. ст. 137),

– преступления против семьи и несовершеннолетних (ст. 150 УК РФ),

– преступления против собственности (ст. 158, 159, 159^3, 159^6, 163, 165 УК РФ),

– преступления в сфере экономической деятельности (ст. 174, 174^1, 180, 186, 187 УК РФ),

– преступления против общественной безопасности (ч. 4 ст. 205–205^5, ст. 207-207^3, 222, 222^1, 226, 226^1 УК РФ),

– преступления против здоровья населения и общественной нравственности (ст.228, 228[1], 230, 234, 242-242[2] УК РФ),

– преступления против основ конституционного строя и безопасности государства (ст. 280, 2801, 282–282[4] УК РФ),

– преступления против правосудия (ст. 296, 298–298[1] УК РФ),

– преступления против порядка управления (ст. 319 УК РФ),

– преступления против мира и безопасности человечества (ст. 354[1] УК РФ).

– иные преступления, связанные с атаками на системы с использованием ИИ (разработка адаптивного вредоносного ПО, автоматизация атак); компрометация цепочек поставок программного обеспечения (Supply Chain Attacks), Deepfake-мошенничество (подделка видео/аудио для вымогательства, дискредитации); преступления в метавселенных и с использованием NFT.

В качестве основных характеристик цифровой преступности выделяются:

1. Трансграничность, поскольку преступник, жертва и инфраструктура могут находиться в разных странах. И**сполнители, инфраструктура, жертвы, финансовые потоки и последствия** пересекают государственные границы, что создает огромные **препятствия для расследования** из-за проблем с юрисдикцией и необходимостью сложной международной координации.

Нами выделяются три основных аспекта трансграничности:

технический, который позволяет организовывать кибер-атаки, преступные сети, вербовать посредников (дропперов) через интернет-ресурсы с последующей оплатой в криптовалюте, использовать зарубежные колл-центры для реализации дистанционных мошеннических схем или склонения граждан к диверсиям. По данным МВД РФ в 2024 году было зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что составило 40% от общего числа преступлений. Ущерб составил 170 млрд. рублей [5]. Сравнение количества совершенных преступлений такого рода за 2021–2024 годы свидетельствует о наличии динамики их роста. Так, в 2024 году рост составил 13.1%. в 2023 году – 29.7%, в 2022 году в сравнении с 2014 годом количество преступлений возросло в 50 раз.

Финансовый аспект, который связан с прибыльностью киберпреступлений. Так, за последние 5 лет финансовый ущерб составил порядка 500 млрд. рублей, в 2023 году – 156 млрд рублей. За последние три года из России за границу было выведено более **350 млрд рублей,** полученных преступным путем, через криптовалюты и анонимные платежные системы. Несмотря на то, что дистанционные хищения остаются лидерами в общей структуре ИТ-преступлений, появился новый способ заработка преступников – продажа персональных пользовательских сведений и несанкционированный доступ к информсистемам. Так, с декабря 2023 по февраль 2024 года, т.е. за 3 месяца, по данным «Лаборатории Касперского» зафиксирован шестикратный рост DDoS-атак по сравнению со значением 2022–2023 года [6].

Правовой аспект, который связан с пробелами в юрисдикциях, отсутствием единых международных норм квалификации ITпреступлений и конфликтов национальных законов, сложностью в сборе доказательств: цифровые следы (логи серверов, IP-адреса) распределены по разным юрисдикциям, что требует длительных процедур взаимодействия между государствами. Не все страны имеют соглашения о правовой помощи или эффективные механизмы взаимодействия правоохранительных органов. Некоторые страны могут сознательно укрывать киберпреступников. Особенно это характерно для стран с коррумпированными властями, слабым киберзаконодательством, которые не желают сотрудничать и становятся пристанищем для хакерских группировок.

Более того, существует насущная потребность в принятии постановления Пленума Верховного Суда РФ по вопросам, связанным с квалификацией преступлений, совершенных с использованием цифровых технологий.

2. Высокая латентность в силу сложности обнаружения факта преступления и идентификации злоумышленника проявляется в следующих ключевых аспектах:

– неочевидность для жертвы, когда факт утечка данных через скрытый бэкдор осуществляется длительное время или шпионское ПО, которое работает незаметно, без явных симптомов и др.

– скрытность действий со стороны преступников посредством использования прокси-сетей для скрытия IP-адресов или использование для переговоров зашифрованных мессенджерах (Telegram, Wickr, даркнет), а также стирание следов с использованием автоматического удаления логов, использование блокчейна для транзакций (Monero, Zcash) или DDoS из ботнета с тысячами устройств в разных странах, что усложняет идентификацию источника. Существует черный рынок киберпреступных услуг (продажа эксплойтов, аренда ботнетов, фишинговые наборы), доступный злоумышленникам по всему миру.

– Недобросовестность пострадавших, когда банки, компании умалчивают о кибер-инцидентах из-за боязни репутационных рисков и потери клиентов. Более того, бизнес не верит в эффективность расследований, и заявления в правоохранительные органы не подаются.

– IT неграмотность пострадавших, когда жертва мошенничества считает утерю финансовых средств своей ошибкой или когда не ведется мониторинг состояния серверов, жертвы не ведут мониторинг.

3. Правовые пробелы, которые прежде всего связаны с отставанием уголовного законодательства от темпов развития цифровой действительности. Новые методы, к примеру, криптоджекинг, не подпадает под статьи УК, а преступления в даркнете не фиксируются правоохранительными органами. Так, фиксируется примерно 10–15% от реального количества совершенных киберпреступлений, что ведет к искажению статистики и безнаказанности киберпреступников, что, в свою очередь, провоцирует повторяемостиь кибератак.

Более того, преступные IT-группировки носят международный характер, когда члены одной хакерской группы находятся в разных странах: одни пишут вредоносный код, другие – ищут уязвимости системы, третьи занимаются обналичиванием средств, добытых преступным путем. Такие группировки могут привлекаться государствами (APT-Advanced Persistent Threat группы) против других стран (правительственных учреждений, корпораций, критической инфраструктуры) для хищения государственных секретов, промышленного шпионажа или дестабилизации.

4. Технологичность (зависимость от сложных ИТ-инструментов, эксплуатация уязвимостей, социальная инженерия).

5. Динамичность и адаптивность к мерам защиты; масштабируемость по причиненном ущербу (вредоносное ПО может поразить миллионы устройств по всему миру); анонимность: использование криптовалют, анонимизирующих сетей, поддельных идентификаторов.

Адаптивность способов совершения цифровых преступлений может проявляться:

– в преступной услуге: модель «Преступление как услуга». Существует рынок специализированных криминальных услуг (аренда ботнетов, продажа эксплойтов, услуги по отмыванию криптовалют, доступ к взломанным корпоративным сетям), что позволяет технически неподготовленным лицам организовывать совершение IT–преступления. Организованы цепи поставок вредоносного ПО: от разработчиков эксплойтов до распространителей (аффилиатов) и операторов инфраструктуры командования и управления (C&C).

– В использовании методик социальной инженерии для манипулирования жертвами людьми остается ключевым способом обхода технических средств защиты (фишинг, претекстинг, байтинг). Эффективным способом воздействия остается способ двойного шантажа (Double Extortion), когда программа-вымогатель шифрует данные, предварительно их похитив, при этом угрожая публикацией в случае неуплаты выкупа.

– В сложности установления места совершения преступления, связанном с технологическим отставанием правоохранителей от уровня, используемого преступниками инструментов и тактик, нехваткой высококвалифицированных кадров и недофинансированием приобретения современных инструментов цифровой криминалистики и разведки.

Таким образом, преступность в цифре представляет собой динамичную, высокотехнологичную и глобально организованную угрозу, наносящую колоссальный экономический и социальный ущерб государству. Ее эволюция напрямую связана с развитием новых технологий, которые преступники адаптируют быстрее, чем системы защиты и правового реагирования. Традиционные методы борьбы с преступностью в цифровой среде оказываются недостаточно эффективными.

Заключение. Успешное противодействие требует комплексного подхода:

1. Модернизация уголовного законодательства посредством создания правовых норм, охватывающих новые угрозы, и процедур работы с цифровыми доказательствами.

2. Оснащение правоохранительных органов передовыми инструментами цифровой криминалистики, киберразведки и прогнозной аналитики и подготовка специалистов новой формации: киберследователей, аналитиков, экспертов.

3. Развитие публично-частного партнерства посредством взаимодействия государства с IT-компаниями в области обмена информацией о киберугрозах в целях быстрого реагирования на инциденты.

4. Повышение цифровой грамотности и кибергигиены как населения, так и сотрудников организаций.

Список литературы

1. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. М.: Юридическая литература, 1991. 160 с.

2. Григорьева А.Е., Петрова Ю.М. О развитии понятия "цифровая преступность» по материалам международных договоров и соглашений // Аграрное и земельное право. 2023. № 12(228). С. 216–218.

3. Доровских Л.А. Преступления в сфере высоких технологий // Киберпреступность. 2016. № 4 (28). С. 240–243.

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

5. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2024 года. [Электронный ресурс]. URL: https://мвд.рф/reports/item/60248328 (дата обращения: 10.08.2025).

6. Лаборатория Касперского (Kaspersky). [Электронный ресурс]. URL: https://www.tadviser.ru/index.php (дата обращения: 02.08.2025).

7. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере: Монография. М.: Российский государственный университет правосудия, 2016. 316 с.

8. Конев Д.А. Криминологическая безопасность и ее обеспечение в сфере цифровых технологий. Дис. …канд. юрид. наук. Омск, 2022. 206 с.

9. Чирков Д.К., Саркисян А.Д. Преступность в сфере высоких технологий: тенденции и перспективы // Национальная безопасность. 2013. № 1 (24). С. 25–32.

УДК 343.2/.7 (075.8)

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

О применении нового варианта статьи 238 УК РФ в отношении медицинских работников в цифровом поле

Аннотация. Целью исследования предлагаемой статьи является анализ нового варианта статьи 238 УК РФ применительно к медицинским работникам под призмой цифрового поля. В декабре 2024 года статья 238 УК РФ обновилась примечанием, уточняющим, что под данную статью не подпадают случаи оказания медицинскими работниками медицинской помощи. Новое примечание породило множество интерпретаций рассматриваемой уголовно-правовой нормы. К примеру, как может показаться в первом приближении, является полное освобождение от уголовной ответственности медицинских работников при оказании ими медицинской помощи. Рассматривая новую редакцию статьи 238 УК РФ с точностью предположить, как будет складываться правоприменительная практика, пока довольно сложно.

Ключевые слова: ст. 238 УК РФ, ятрогенные преступления в цифровом поле, уголовная ответственность медицинского работника, медицинский работник в уголовном праве, медицинская помощь в уголовном праве

Y.Y. Malysheva,
candidate of Law, Associate Professor,
Kazan Institute (branch) of the All-Russian State
University of Justice (RPA of the Ministry of Justice of Russia)

On the application of new option of article 238 of the RF Criminal Code in relation to medical workers in the digital space

Abstract. The purpose of the study of the proposed article is to analyze the new version of Art. 238 of the Criminal Code of the Russian Federation in relation to medical workers under the prism of the digital field. In December 2024 Art. 238 of the Criminal Code of the Russian Federation was updated with a note clarifying that this article does not cover cases of medical care provided by medical workers. The new note has given rise to many interpretations of the criminal law norm in question. For example, as it may seem at a first approximation, there is a complete exemption from criminal liability for medical workers when they provide medical care. Considering the new edition of Art. 238 of the Criminal Code, it is still quite difficult to accurately predict how law enforcement practice will develop.

Keywords: Art. 238 of the Criminal Code of the Russian Federation, iatrogenic crimes in the digital field, criminal liability of a medical worker, medical worker in criminal law, medical assistance in criminal law.

Введение. Априори статья 238 УК РФ относится к «ятрогенным преступлениям», когда ошибка в действии (бездействии) медицинского работника приводит к необратимым преступным последствиям [1. С.331]. В принципе, ошибочное поведение врача, по сути, не должно приводить к преступлению, поэтому употребление термина «ятрогенные преступления», на наш взгляд, представляется необоснованным и не вполне корректным. Применение статьи 238 УК РФ в цифровом пространстве сегодня является весьма актуальным, поскольку возможности медицины и телемедицины в разгаре XXI века позволяют оказывать как медицинскую помощь, так и медицинские услуги в цифровом поле, включая корректировку лечения и консультации онлайн, к примеру, в период пандемии COVID-19 или при невозможности личного обращения пациента к лечащему врачу.

Основная часть. В декабре 2024 г. Федеральным законом от № 514-ФЗ статья 238 УК РФ была дополнена примечанием о том, что под данную статью не подпадают случаи оказания медицинскими работниками медицинской помощи [2. С.24]. Данная позиция законодателя звучит весьма обнадеживающе. Потому новым в вопросе уголовной ответственности по статье 238 УК РФ, как может показаться в первом приближении, является полное освобождение от уголовной ответственности медицинских работников при оказании ими медицинской помощи онлайн и оффлайн.

Хотелось бы отметить, что с момента реализации привлечения к уголовной ответственности врачей по статье 238 УК РФ к медицинским работникам наблюдалась следующая тенденция. Изначально те общественно опасные последствия, которые возникали в результате оказания платных медицинских услуг, квалифицировались по статье 238 УК РФ. При этом медицинская помощь, предоставленная в рамках системы ОМС, при наличии тех же последствий влекла за собой ответственность по другим статьям УК РФ. Однако со временем это негласное правило перестало соблюдаться, и правоприменительная практика стала идти по пути квалификации случаев оказания медицинских услуг, не отвечающих требованиям безопасности жизни и здоровья пациента в рамках ОМС, также по статье 238 УК РФ [3. С.155].

Статья 238 УК РФ при применении ее к медицинским работникам вступает в противоречие с обобщенной судебной практикой. Поэтому по обновленному этапу правового регулирования как раз и было добавлено необходимое примечание к статье 238 УК РФ [7. С.71]. Мы тем не менее понимаем, что в будущем могут возникнуть множественные нюансы правоприменения, требующие дополнительных разъяснений и законодательного регулирования [8. С.199]. Так, статья 238 УК РФ имеет более продолжительный срок давности совершения преступления, который составляет шесть лет. Все остальные ятрогенные преступления относятся к числу преступлений небольшой тяжести, кроме части 2 статьи 235 УК РФ, срок давности по которым

составляет два года. Поскольку расследование ятрогенных преступлений занимает значительное время с учетом проведения судебно-медицинских экспертиз, то следствие и суд могут не уложиться в отведенный срок два года [6. С.144]. Поэтому скорее всего надо ждать ужесточения по имеющимся «ятрогенным статьям» [3. С.91].

Приведем подходящий как нельзя лучше пример из судебной практики.

27 января Черновский суд в закрытом судебном заседании признал врача ГБУЗ «Станция скорой медицинской помощи», а также врача ГУЗ «Краевая клиническая инфекционная больница» виновными в гибели годовалого ребенка. По версии следствия 7 января 2023 года жительница Улетовского района обратилась в инфекционную больницу с жалобами на температуру и расстройство ЖКТ у годовалой дочери. Врач-стажер, находясь на дежурстве в модульном инфекционном отделении ГУЗ «Краевая клиническая инфекционная больница», недооценила состояние тяжести ребенка, не пригласила для осмотра дежурного врача, работающего с ней в одну смену, имеющего значительный стаж и опыт в диагностике и лечении инфекционных болезней, приняла решение проводить самостоятельный прием ребенка, оказывая таким образом, медицинские услуги ненадлежащего качества лицу, не достигшему возраста 6 лет, имея при этом реальную возможность предоставить своевременную квалифицированную помощь и не допустить развитие смертельных осложнений малолетнего пациента. В 2023 году действительно даже оказание бесплатной медицинской помощи расценивалось как оказание услуги врачом. Ребенок не был госпитализирован, было назначено лечение на дому. 8 января 2023 года в связи с ухудшением состояния ребенка родители обратились по месту жительства в ФГКУ «321 Военный клинический госпиталь», откуда врач анестезиолог-реаниматолог вызвал скорую медицинскую помощь. Врач – анестезиолог-реаниматолог ГБУЗ «Станция скорой медицинской помощи» по приезду оценила состояние ребенка как крайне тяжелое, критическое, представляющее угрозу для жизни, однако приняла решение не оказывать экстренную помощь, а начать эвакуацию пациента в инфекционный стационар без проведения интенсивной терапии. Сразу по поступлении в отделение реанимации ГУЗ «Краевая клиническая инфекционная больница», несмотря на реанимационные мероприятия, наступила смерть ребенка.

В данном конкретном примере дефекты оказания медицинской помощи врачами состоят в прямой причинно-следственной связи с наступлением смерти ребенка. При условии проведения полноценного лечения состояние было полностью обратимым, у девочки имелись все шансы на выживание [10. С.250].

Органами предварительного следствия врачам было предъявлено обвинение в совершении преступления, предусмотренного пунктами «б» и «в» части 2 статьи 238 УК РФ – оказание услуг, не отвечающих требованиям безопасности жизни и здоровья потребителей, если они совершены в отношении услуг, предназначенных для детей в возрасте до 6 лет и повлекли по неосторожности причинение тяжкого вреда здоровью и смерть человека [4. С.194]. В судебном заседании подсудимые свою вину не признали.

С учетом последних изменений в уголовном законодательстве, внесенных Федеральным законом от 28 декабря 2024 г. № 514-ФЗ, действия подсудимых судом переквалифицированы на часть 2 статьи 109 УК РФ – причинение смерти по неосторожности вследствие ненадлежащего исполнения своих профессиональных обязанностей [9. С. 94].

Суд назначил каждой осужденной наказание в виде ограничения свободы на срок 2 года с лишением права заниматься врачебной деятельностью на срок 2 года. В пользу родителей с медицинских учреждений взыскана компенсация морального вреда в размере 2 000 000 рублей, а также материальный ущерб в размере 96 000 рублей. В связи с истечением срока давности уголовного преследования осужденные освобождены от наказания. Приговор так и не вступил в законную силу.

В июле 2025 года в Уфе возбуждено уголовное дело по статье 238 УК РФ, суть дела следующая. Пенсионера, который находился в пансионате для пожилых людей, замотали в простыни и связали. Подобные события в уфимском учреждении «Печки-лавочки» для престарелых клиентов являются регулярной практикой, как следует из материалов уголовного дела. Пожилых людей в данном Доме престарелых избивают, морят голодом, в особенности тех, кто высказывает недовольство. Кроме того, выяснилось, что в пансионате полная антисанитария, живут клопы и тараканы. Медицинская помощь в подобных учреждениях не оказывается, поэтому очевидно возбуждение уголовного дела именно по изучаемой нами уголовно-правовой норме.

Заключение. Рассматривая новый вариант статьи 238 УК РФ, спрогнозировать с точностью, как будет складываться правоприменительная практика, пока довольно сложно [5. С. 415]. Сегодня стоит учитывать и широкие возможность применения рассматриваемой уголовно-правовой нормы и оффлайн, и в цифровом поле одновременно, поскольку для консультаций онлайн с целью корректировки ранее назначенного лечения это является допустимым.

Список литературы

1. Ахметгалеева А. Ф. Теоретические аспекты и особенности правоприменительной практики при привлечении медицинских работников к уголовной ответственности за совершение преступлений, предусмотренных статьей 238 Уголовного кодекса Российской Федерации // Вестник Удмуртского университета. Серия Экономика и право. 2019. Т. 29, № 3. С. 329-342. EDN EKINDZ.

2. Быкова Е. Г., Казаков А. А. Отдельные правовые и процессуальные риски оценки ненадлежащего оказания медицинских услуг по ст. 238 УК РФ // Проблемы расследования уголовных дел о преступлениях, совершенных медицинскими работниками при оказании медицинской помощи : Материалы международной научно-практической конференции, Москва, 28 ноября 2024 года. – Москва: Московская академия следственного комитета, 2025. С. 23-28. EDN TOPWNH.

3. Быкова Е. Г. О доказывании реальной опасности для жизни или здоровья косметологической услуги, оказанной лицом, не имеющим медицинского образования // Судебно-медицинская наука и экспертная практика: задачи, пути совершенствования на современном этапе : Труды IX Всероссийского съезда судебных медиков с международным участием, Москва, 22–24 ноября 2023 года. – Череповец: ИП Мочалов С.В., 2023. С. 154-161. EDN TRCDQM.

4. Малышева Ю. Ю. О границах уголовной ответственности врача-психиатра: актуальные рассуждения // Уголовная политика и правоприменительная практика : Сборник научных статей по результатам работы Всероссийской научно-практической конференции, Санкт-Петербург, 01 ноября 2024 года. – Санкт-Петербург: Центр научно-информационных технологий "Астерион", 2025. С. 193-196. EDN HAYYYS.

5. Малышева Ю. Ю. Безгранична ли уголовная ответственность врача-психиатра? // Обеспечение безопасности современного общества и государства в условиях многополярного мира : Сборник материалов X Международной научно-практической конференции, Чебоксары, 17–19 апреля 2025 года. Чебоксары: Чувашский государственный университет им. И.Н. Ульянова, 2025. С. 413-417. EDN GBWFGE.

6. Малышева Ю. Ю. Уголовно-правовые и криминологические аспекты служебного подлога в медицинской деятельности / Ю. Ю. Малышева // 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.

7. Малышева Ю. Ю. О перспективах уголовно-правовой охраны медицинских работников в России // Марийский юридический вестник. 2024. – № 3-4(44). С. 70-73. EDN MUOAWJ.

8. Малышева Ю. Ю. Врачебные ошибки и "вина" пациента под призмой цифровых технологий / Ю. Ю. Малышева // Цифровые технологии и право : Сборник научных трудов II Международной научно-практической конференции: в 6 томах, Казань, 22 сентября 2023 года. Казань: Издательство "Познание", 2023. С. 197-202. EDN JHAMAS.

9. Малышева Ю. Ю., Малышев В. К. Уголовно-правовые аспекты врачебных ошибок в соотношении с «виной» пациента // Вестник Волжского университета им. В.Н. Татищева. 2023. Т. 2, № 4(106). С. 90-99. DOI 10.51965/2076-7919_2023_2_4_90. EDN FDQHYK.

10. Шпаков А. С. Проблематика вины в статье 238 Уголовного кодекса Российской Федерации ее влияние на выбор смежных норм // Проблемы становления гражданского общества: электронный сборник статей Международной научной студенческой конференции. В 2-х частях, Иркутск, 24 марта 2023 года. Том Часть II. – Иркутск: Иркутский юридический институт (филиал) федерального государственного казенного образовательного учреждения высшего образования "Университет прокуратуры Российской Федерации", 2023. С. 249-252. EDN NHVHFO.

УДК 343.1

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

Цифровая трансформация уголовного дела (уголовного производства): опыт внедрения зарубежных электронный систем в уголовное судопроизводство

Аннотация. В настоящей статье рассмотрен опыт некоторых государств, внедряющих как элементы электронного уголовного дела в досудебной стадии уголовного судопроизводства, так и в целом полный переход на цифровые площадки, заменяющие собой бумажное уголовное дело в привычном виде, рассмотрены положительные моменты, а также проблемы, которые выявлены участниками отношений в сфере уголовного процесса, приведены результаты опроса непосредственных участников уголовно-процессуальных отношений (следователей, адвокатов).

Ключевые слова: цифровые технологии; электронное уголовное дело; электронное судопроизводство; электронное правосудие; модуль уголовного дела; портал уголовного дела

R. N. Malyshkin,
Candidate of Law,
Kazan Innovative University named after V.G. Timiryasov

Digital transformation of a criminal case (criminal proceedings): experience in implementing foreign electronic systems in criminal proceedings

Abstract. This article attempts to review the experience of some countries that have implemented both elements of electronic criminal cases in the pre-trial stage of criminal proceedings, as well as a complete transition to digital platforms that replace traditional paper criminal cases. The article examines the positive aspects and challenges identified by participants in the criminal process, and presents the results of a survey conducted among direct participants in criminal proceedings (investigators and lawyers).

Keywords: digital technologies; electronic criminal case; electronic legal proceedings; electronic justice; criminal case module; criminal case portal

Введение

Цифровизацией всех сфер государственного управления сейчас уже никого не удивить. Практически во всех странах в стратегию развития управления заложена большая часть бюджетных и иных ресурсных расходов на переход в регулирование работы государственного аппарата в электронной среде. Система правосудия не

остается в стороне. Однако, если работа судов цифровизируется уже не один десяток лет, то уголовное производство, в частности досудебное производство по уголовным делам, в разных странах в электронном виде формируется постепенно. Примечательным является то, что цифровые платформы и новые форматы расследования уголовных дел с применением формы электронного уголовного дела не побоялись внедрять именно молодые страны, где опыт своей уголовно-процессуальной правовой системы невелик. В Российской Федерации с ее почтенной историей развития и формирования уголовного процесса как отрасли российского права, переход к новому формату – электронной системе уголовного дела еще предстоит пройти. Опыт передовых стран в области применения формата электронного уголовного дела помог бы избежать ошибок, допущенных другими, совершенствовать свою собственную правовую систему и улучшить эффективность работы уголовно-процессуальной деятельности органов предварительного расследования и суда.

Основная часть

Всеобщее стремление правительств стран Европы к цифровизации процессов в системе уголовного правосудия продиктовано целями всеобщей информатизации государственного регулирования. Впрочем, как и во всем мире. Отличие в развитии таких систем обусловлено различием правовой (законодательной) системы и финансовыми возможностями. Часть стран готова к радикальным изменениям, вплоть до резкого перехода к цифровым платформам и изменению законодательства в уголовно-процессуальной отрасли, другая, большая часть стран, идет по пути мягкого, постепенно перехода [5. С.272]. В России понятия электронного уголовного дела пока не закреплено, как и нет четкого понимания в чем разница между электронным делом и цифровым уголовным делом. Хочется отметить, что и самого понятия «уголовное дело» нигде не закреплено. С.В. Зуев представляет свое собственное определение «Электронное уголовное дело – совокупность документов, представленных участниками уголовного судопроизводства или информационной системой в электронно-цифровой форме, размещенных на цифровой платформе в едином модуле осуществления производства по уголовному делу с применением информационных технологий в соответствии с требованиями УПК РФ» [2. С. 83]. Данное определение весьма удачно. Оно также одновременно раскрывает и понятие «уголовное дело», под которым можно понимать результаты осуществления уголовного судопроизводства. Ученый выработал план, в котором предложил развитие отечественного уголовного судопроизводства в электронном виде двумя путями: разработки и внесение в УПК РФ отдельной главы, то есть интеграция в действующее уголовно-процессуальное законодательство; и второй – создание кардинально нового уголовно-процессуального кодекса, который будет базисом для электронного уголовного дела. Оба варианта имеют свои достоинства, но, чтобы принять стратегию развития системы электронного правосудия в России было бы полезно изучить опыт других государств.

Основываясь на исследовании, проведенном рядом европейских ученых Ален Пьетрикс Сипма, Каролин де Блок и Дирк Питер Ван Донк, сделанном в 2020 году [7. С. 442] были выявлены основные причины цифровизации уголовного судопроизводства.

Так Англия руководствовалась экономическими соображениями и в числе причин указала сокращение бюджета на всех этапах организационного управления, в том числе и в области обеспечения безопасности и правопорядка. Это возможно сделать, по их мнению, при помощи перехода к цифровизации уголовного судопроизводства. Программа реализуется с 2010 года.

В Австрии руководствовались необходимостью в более эффективных методах регулирования в области правосудия. Начало реформ – 1989 г.

В Дании в числе основных причин видится цифровизация всех сфер государственного управления и регулирования. Начало реформ – 2005 г.

В Эстонии все объяснялось необходимостью прозрачности государственного управления. Стоит отметить, что Эстония является одним из лидеров цифровизации государственного управления в Европе (3 место по данным ООН) [4. С.61] Начало реформирования – 2004г.

Основные цели цифровой трансформации уголовного судопроизводства в этих же странах:

Англия – повышение эффективности систем правосудия;

Австрия – улучшение поддержки специалистов уголовно-процессуальной деятельности, работающих уголовными делами;

Дания – передача информации в цифровом виде (здесь видимо понимается о сохранении информации в цифровом виде)

Эстония – улучшение качества работы системы правосудия и защита прав граждан.

Во всех перечисленных странах оцифровке подлежит все дело, но в суд материалы могут быть представлены: как одновременно в бумажном и цифровом (Австрия Дания), так и чисто в цифровом виде (Англия, Эстония).

В Швейцарии также электронное уголовное дело является лишь частичным, где основные процессуальные действия остаются в бумажном виде и в последующем оцифровываются [6. С. 465].

В Австрии система отхода от бумажного уголовного производства не потребовала отказа от прежнего законодательного регулирования, она вполне уложилась в существующую систему лишь частично ее дополнив рядом норм. Таким образом представленный вариант некоторых исследователей о том, что внедрение электронного уголовного дела потребует полную замену УПК РФ [2. С. 83], на наш взгляд можно избежать.

Однако такой способ интеграции в существующую правовую систему без его кардинального изменения объясняется двумя причинами: во-первых, как ране было

указано, длительностью внедрения цифровизации и параллельного развития вместе с законодательным закреплением. Во-вторых, в Австрии уголовное дело не ведется полностью в электронном виде, а лишь происходит оцифровка бумажных документов и собирание дела в единую папку. Документооборот между органами власти пока тоже не налажен полностью и какие-то документы передаются при межведомственном сообщении в бумажном виде. Таким образом видим, что это не является электронным уголовным процессом в том виде, которое предлагается нами.

Основные проблемы, которые выявлены в проанализированных правовых системах электронного уголовного дела.

Общей проблемой, если так можно выразиться, для всех правовых систем является стремительное развитие права. Изменения законодательства требует оперативного изменения и программного обеспечения электронных сервисов (баз данных, цифровых площадок оказания цифровых услуг). То есть во всех правовых цифровых системах невозможно предусмотреть заранее гибкой системы, которая бы оперативно вносила бы изменения в платформу электронного уголовного дела.

Система электронного подписания документов. В некоторых странах до сих пор отмечаются трудности с подписанием (заверением) документов, составляемых на месте, то есть при совершении непосредственных следственных действий. Если при отправке цифровых жалоб, ходатайств, заявлений в органы власти это решаемо путем электронной цифровой подписи через соответствующий сервис, то в «поле» при работе на местности (месте происшествия) могут возникать затруднения. Однако это также можно решить путем предоставления возможности расписывания в электронном планшете участником следственного действия. То есть, когда участник берет стилус и расписывается на экране электронного устройства. При разработке соответствующего программного обеспечения подготовки процессуальных документов должна быть предусмотрена такая функция как электронно-графическая подпись (ЭГП). Интересен опыт Англии, где так называемая «живая» подпись не проставляется. ««Фактическая «мокрая подпись» нигде не требовалась в таком виде. […] Мы начали работать в цифровом формате без каких-либо подписанных свидетелями заявлений. И до сих пор это ни разу не оспаривалось» [7. С.440]. Довольно-таки смелый шаг, который, на наш взгляд, пока рано внедрять в наше судопроизводство, учитывая особенности нашего менталитета доверять рукописным документам и подписям.

В некоторых странах, например в Дании, проблемой все еще остается то, что развитие цифровой среды является задачей каждого органа, задействованного в уголовном судопроизводстве, в отдельности. Это не единая система, а лишь взаимодействующие друг с другом базы. Скоординированность работы в этом процессе заметно улучшила эффективность.

В Англии, поскольку процесс цифровизации производства по уголовным делам начался с 2010 года эта проблема была решена. Несмотря на то, что в электронное производство включены разные, независимые друг от друга органы, им удалось

наладить совместную работу и обмен документами, обеспечивающие доступ к смежным и внешним базам данных, которые в совокупности обеспечивают эффективное расследование, рассмотрение и разрешение уголовных дел.

Интересен опыт внедрения цифровых систем в уголовном процессе в странах ближнего зарубежья. Практически везде внедряется система электронного правосудия. Распределение дел, регистрация и систематизация судебного производства уже является обыденным явлением во всех странах ближнего зарубежья – стран Евразийского правового пространства. В тех странах, где такое правосудие действует с начала 2000-х, уже внедряются новые механизмы, способные на основе алгоритмов использования искусственного интеллекта (ИИ) помогать суду в определении оптимального наказания. Так Х.Д. Алекберов из Азербайджана разработал представил к внедрению «Электронные весы правосудия», то есть концепцию электронной системы определения виновному оптимальной меры наказания с учетом объективных и субъективных свойств, совершенного им преступления» [1. С. 60].

Передовой опыт цифровизации судопроизводства в странах Евразийского союза показывает, что резкий переход к электронному правосудию выявил сразу две ключевые проблемы: технические сложности с нехваткой серверов для обработки информации и субъективные – отсутствие подготовленного персонала и недостаточная цифровая грамотность населения – участников правовых отношений [5. С. 59]. Примечательно, что электронное уголовное дело как форма в Казахстане действует с 2017 года. Уже сейчас можно говорить об успешном опыте его применения и положительных результатах. Так электронная система уголовного дела предусматривает электронное сопровождение от начальной стадии принятия сообщения о преступлении до конечной стадии – исполнение наказания. В ходе применения электронного уголовного дела были внедрены ряд полезных сервисов, которые контролируют, время следственных действий (в том числе допросов по продолжительности), место производства следственных действий с записью. Все это приводит к сокращению нарушений прав участников уголовного судопроизводства, таких как нарушение сроков при производстве допросов, незаконных задержаний [3. С. 34].

В целом анализ показывает, что развитие системы электронного уголовного производства идет двумя путями: оцифровывание электронного уголовного дела и связанных с ним бумажных документов (как полное, так и частичное) и полностью цифровизация.

Учитывая изученные системы электронного уголовного дела, можем выделить ряд положительных моментов, которые могут быть реализованы в отечественной платформе.

Цифровое (электронное) уголовное дело поможет решить ряд существующих проблем. В частности, не процессуальные, решения лиц, осуществляющих расследование, уполномоченных на принятие решений по делу. Программа,

автоматически будет блокировать действия, противоречащие уголовно-процессуальному закону и подсказывать возможные варианты. Это не только улучшит качество предварительного расследования, но и снизит нагрузку на суды, которые вынуждены рассматривать жалобы участников процесса в порядке с 125 статьи УПК РФ.

Проведенный опрос ключевых участников уголовного судопроизводства показал, что электронное уголовное дело рано или поздно нужно будет внедрять в уголовный процесс. В ходе беседы, поначалу как следователи, так и адвокаты были резко против внедрения электронного уголовного дела. Следователи свой скептицизм объясняли нежеланием что-то менять, дополнительной нагрузкой на следователя за счет того, что придется вести двойное уголовное дело в бумажном виде и в виде электронного дубликата. Высказывались опасения по поводу необходимости дополнительного обучения по работе с цифровой площадкой, неизбежными ошибками в работе системы как технического плана, так и из-за неграмотности сотрудников. Адвокаты же в числе причин неприятия внедрения указывали отсутствие доверия к прозрачности контроля за технической стороной процесса. Однако, когда участникам опроса было предложено перечислить положительные стороны во внедрении электронного уголовного дела, то следователи указали на сокращение рутинной работы с документами, которая присутствует в бумажном виде. Это опись и подшивание дел, быстрый доступ к материалам всех процессуальных участников, который может заменить необходимость выделения большого объема времени на ознакомление с материалами дела потерпевшего, защитника, подозреваемого/обвиняемого. Адвокаты сообщили, что при использовании технологии блокчейна будет невозможно без оставления следов внести изменения в материалы уголовного дала. Таким образом будет исключена возможность фальсификации доказательств путем подмены документов их последующим изменением. Быстрый доступ в режиме реального времени к материалам уголовного дела, копии которых может получить адвокат также являются плюсом такой формы. Возможность подачи жалобы, ходатайства также упрощается. Так, например, при подачи электронной жалобы в самой системе не нужно будет распечатывать и заново оцифровывать обжалуемый документ. Достаточно указать на номер файла (страницу дела), и система подгрузит документ автоматически. Время подачи жалобы (ходатайства) также будет вспомогательным элементом при соблюдении сроков. Система может оповещать о находящихся в производстве делах, истекающих сроках. Опыт Казахстана во внедрении системы контроля времени допросов, иных следственных действий также может быть учтен. Некоторыми участниками, которым приходиться выступать на стороне защиты, выдвинуто предложение учитывать в системе геолокацию устройства, с помощью которого производиться введение данных о производстве следственного действия. Таким образом можно отслеживать не только время, но и место проведения следственного действия.

В итоге ключевые участники уголовного процесса пришли к выводу о том, что электронное уголовное дело может существенно облегчить работу как следователей, так и адвокатов. Также это будет существенным дополнением к системе надзора за расследованием уголовных дел.

Заключение

Подводя итог проведенному исследованию, делаем вывод, что внедрение электронного уголовного дела – есть необходимость в современных реалиях. Опыт цифровизации уголовного судопроизводства других стран очень важен. Анализ слабых мест цифровых площадок, ошибок в администрировании процесса цифровизации поможет обойти их. Произошедшая цифровая трансформация общества, увеличение доказательственного значения цифровых следов преступлений, повсеместное использование де-факто электронных доказательств в практике деятельности правоохранительных органов наталкиваются на проблему отсутствия понятия «электронных доказательств» в уголовно-процессуальном законе [8. С. 272].

На наш взгляд цифровизация уголовного дела – являясь комплексной системой должна выглядеть как цифровая автоматизированная система, полностью включающая в себя все уголовное дело. Это не просто оцифровка бумажного дела и перевод его в электронный формат. Электронное уголовное дело должно включать в себя возможности рассмотрения от самого начала, например обращения (заявления) потерпевшего в цифровом формате, до исполнения приговора, когда информация сопровождается и отображается в электронном формате в учреждения исполнения наказания (орган принудительного исполнения).

В разработке проекта необходимо учесть мнение непосредственных участников уголовно-процессуальных отношений. Это можно сделать и путем публичного опубликования проекта закона о внедрении электронного уголовного дела, как это было реализовано в 2010 году с проектом Федерального закона «О полиции». В свое время это позволило учесть мнение и интересы всех категорий граждан, политиков, ученых, экспертов и простых граждан страны. Такой подход позволит уже на стадии разработки цифровой платформы учесть моменты, которые улучшат ее работу. Открытость и публичность рассмотрения законопроекта также ознакомит граждан с внедряемыми технологиями в интересах защиты их прав и свобод, а также обеспечит сопричастность граждан к правотворческому процессу.

Список литературы

1. Аликперов Х. Д. Электронная технология определения оптимальной меры наказания («Электронные весы правосудия») // Российский судья. 2020. №. 4. С. 59-64.

2. Зуев С. В., Моругина Н. А. Электронное уголовное дело: теоретическая модель // Вестник Казанского юридического института МВД России. 2024. Т. 15. №. 3 (57). С. 83-94.

3. Тлеубаев Д. К., Иманбаев С. М., Карымсаков Р. Ш. Цифровизация уголовного процесса в Республике Казахстан: становление и практика применения //Colloquium-journal. – Голопристанський міськрайонний центр зайнятості, 2021. №. 11 (98). С. 31-37.

4. Щепотин А. В. Основные направления цифровизации судопроизводства и правосудия в государствах евразийского правового пространства // Вестник Таганрогского института управления и экономики. 2025. Т. 1. С. 58-63.

5. Bisschop L., Hendlin Y., Jaspers J. Designed to break: planned obsolescence as corporate environmental crime //Crime, Law and Social Change. 2022. Т. 78. №. 3. – С. 271-293.

6. 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.

7. Seepma A. P., de Blok C., Van Donk D. P. Designing digital public service supply chains: four country-based cases in criminal justice // Supply Chain Management: An International Journal. 2021. Т. 26. №. 3. С. 418-446.

8. 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. https://doi.org/10.21202/jdtl.2023.11. EDN: SGAOKS

УДК 343.98

А. В. Мишин,
доктор юридических наук, доцент,
Казанский (Приволжский) федеральный университет

Совершенствование применения мер безопасности в отношении участников уголовного судопроизводства в условиях цифровизации

Аннотация. Уголовно-юрисдикционная деятельность по созданию условий для безопасного участия свидетелей, потерпевших и иных участников в производстве по делу как защищаемых лиц в настоящее время неразрывно связана с процессом цифровизации в качестве средства существенного повышения конфиденциальности указанных участников. Обеспечение безопасности защищаемых лиц включает в себя формирование соответствующих уголовно-правовых и криминалистических механизмов, которые должны сопровождаться реализацией цифровых технологий при применении мер государственной защиты по делам, связанным с осуществлением посткриминального противоправного посягательства на участников процесса.

Ключевые слова: уголовное судопроизводство, правоохранительная деятельность, цифровые технологии, государственная защита, защищаемые лица, меры безопасности, процессуальные действия

A. V. Mishin,
Doctor of Law, Docent,
Kazan (Volga Region) Federal University

Improving the application of security measures against participants in criminal proceedings in the context of digitalization

Abstract. Criminal jurisdiction activities aimed at creating conditions for the safe participation of witnesses, victims and other participants in the proceedings as protected persons are currently inextricably linked to the process of digitalization as a means of significantly increasing the confidentiality of these participants. Ensuring the safety of protected persons includes the formation of appropriate criminal law and criminalistic mechanisms, which should be accompanied by the implementation of digital technologies in the application of state protection measures in cases related to the implementation of post-criminal unlawful encroachment on participants in the process.

Keywords: criminal proceedings, law enforcement, digital technologies, state protection, protected persons, security measures, procedural actions

Введение

В настоящее время при производстве по уголовному делу особое значение приобретает внедрение цифровых средств и технологий, призванных повысить

эффективность уголовно-процессуальной деятельности, уровень и качество доказательственного процесса по делу в целом.

Использование цифровых технологий и систем находит свое отражение и при применении мер безопасности в отношении потерпевших, свидетелей и иных участников уголовного процесса, подвергшихся посткриминальному противоправному воздействию. Отметим, что информационные технологии при решении задач обеспечения безопасности таких участников реализуются в различных формах и направлениях. Так, в последние годы следственные и судебные действия с участием защищаемых лиц все чаще проводятся в дистанционном режиме, в том числе с применением систем видеоконференц-связи.

Кроме того, в ходе обмена конфиденциальной информацией по делу посредством цифровых коммуникативных средств (абонентских устройств) следует использовать P2P (peer-to-peer)-соединения, исключающие отправку данных на промежуточные сервера, что позволит не допустить утечки информации в случае взлома или попытки намеренной ее передачи третьим лицам.

Вместе с тем следует прогнозировать наличие определенных рисков применения цифровых средств, которые могут быть обусловлены возникшей следственной или судебной ситуацией. Среди возможных факторов, вызывающих указанные риски, могут быть, например, такие, как нарушение конфиденциальности и тайны следствия; доступ посторонних лиц; искажение данных или их утрата; отсутствие делового взаимодействия между следователем, надзирающим прокурором и судом с сотрудниками подразделения государственной защиты [1. С. 74]. К сожалению, подобные факторы могут негативно повлиять на результаты процесса обеспечения безопасности и достижение цели уголовного судопроизводства.

Применение цифровых технологий и систем в ходе процессуальных действий с участием защищаемых лиц, в частности при допросе, позволяет достичь повышения эффективности обеспечения их безопасности в связи с участием в уголовном деле, а также процесс доказывания в целом.

Применение цифровых средств и технологий востребовано и при производстве иных процессуальных действий, связанных с применением мер безопасности в отношении их участников, а именно контроля и записи телефонных и иных переговоров, получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Заключение

Следует констатировать, что использование цифровых технологий при применении мер безопасности к защищаемым лицам в ходе производства по уголовному делу существенно повышает его результативность. Области применения указанных технологий в настоящее время активно расширяются. В этой связи следует считать целесообразным дополнение действующего УПК РФ отдельными правовыми нормами, регулирующими процедуру применения соответствующих информационных

технологий, что создает необходимость научной разработки соответствующих рекомендаций по их реализации. Процесс цифровизации в этом случае должен быть связан с созданием правовой и нормативной базы, имеющей межотраслевое и комплексное содержание [2. С. 156].

Список литературы

1. Брусницын Л.В. Посткриминальное воздействие и некоторые аспекты участия потерпевших и свидетелей в уголовном процессе // Судебная власть и уголовный процесс, 2018. № 1. С. 71-86.

2. Епихин А.Ю., Мишин А.В. Цифровое обеспечение процесса применения мер безопасности в уголовном судопроизводстве // Юридический вестник ДГУ, 2025. Т. 54, № 2 (74). С. 156-163.

3. Мишин А.В. Частная криминалистическая теория обеспечения безопасности участников уголовного судопроизводства: автореф. дис. … докт. юрид. наук. Казань, 2025. 47 с.

О. В. Обернихина,
преподаватель кафедры уголовно-исполнительного права
и организации исполнения наказаний,
не связанных с изоляцией осужденных от общества
(Кузбасский институт ФСИН России)

Обратная сила уголовного закона и цифровые технологии: проблемы теории и практики

Аннотация. В статье исследуются проблемы применения обратной силы уголовного закона в условиях цифровой трансформации общественных отношений. Автором выделены три ключевых проблемных вопроса: определение момента появления цифровых объектов в качестве предмета преступления, квалификация деяний с участием искусственного интеллекта и применение «цифровых наказаний» к преступлениям прошлого. Проведен анализ мнений ведущих ученых, предложены варианты решений выявленных проблем.

Ключевые слова: обратная сила уголовного закона, цифровизация, киберпреступность, искусственный интеллект, криптовалюта, принцип законности, дифференциация ответственности

RETROACTIVE EFFECT OF CRIMINAL LAW AND DIGITAL TECHNOLOGIES: PROBLEMS OF THEORY AND PRACTICE

Abstract. The article examines the problems of applying the retroactive effect of criminal law in the context of the digital transformation of social relations. The author identifies three key problematic issues: determining the moment of emergence of digital objects as the subject of a crime, qualification of acts involving artificial intelligence, and the application of «digital punishments» to crimes of the past. An analysis of the opinions of leading scholars is carried out, and solutions to the identified problems are proposed.

Keywords: reverse force of criminal law, digitalization, cybercrime, artificial intelligence, cryptocurrency, principle of legality, differentiation of responsibility

Введение. Цифровая трансформация, охватившая все сферы жизни современного общества, ставит перед уголовно-правовой наукой принципиально новые вопросы. Одним из наиболее сложных является проблема применения обратной силы уголовного закона (ст. 10 УК РФ) к отношениям, возникающим в цифровой среде.

Как справедливо отмечают Е.А. Русскевич, А.П. Дмитренко и Н.Г. Кадников, классическая модель уголовного права, сформированная для индустриального общества XX века, переживает кризис в условиях цифровой реальности, что требует переосмысления базовых категорий, включая действие закона во времени [4. С. 591).

Настоящая статья посвящена выявлению проблемных аспектов применения ст. 10 УК РФ к цифровым феноменам и поиску путей их разрешения.

Основная часть. Первая и наиболее очевидная проблема связана с определением того момента, когда те или иные цифровые объекты (криптовалюта, NFT-токены, виртуальное имущество) стали признаваться предметом преступления. Э.Л. Сидоренко обращает внимание на то, что правовое регулирование не всегда успевает за появлением новых цифровых финансовых активов, NFT-токенов и стейблкоинов, а правоприменительная практика сталкивается с трудностями из-за отсутствия понятия цифрового кошелька для наложения ареста и методологии изъятия цифровых доказательств [7].

Анализ мнений ученых по данному вопросу обнаруживает два основных подхода. Сторонники первого подхода (например, О.Ф. Сундурова) полагают, что преступления, совершаемые в условиях цифровизации, обладают повышенной степенью общественной опасности, и ее следует учитывать при привлечении лиц к уголовной ответственности, соответственно, перечень статей с квалифицирующим признаком использования цифровых технологий должен быть расширен [9. С. 132]. Второй подход, представленный Е.А. Русскевичем, заключается в том, что цифровой способ совершения преступления далеко не всегда свидетельствует об увеличении общественной опасности деяния, а дополнение закона указанием на использование сети Интернет должно компенсировать реально сложившийся разрыв в степени опасности, а не создавать «цифровых двойников» традиционных запретов [5, С. 30].

Представляется, что позиция О.Ф. Сундуровой, при всей ее привлекательности с точки зрения усиления борьбы с киберпреступностью, несет в себе риск нарушения правила об обратной силе уголовного закона. Если законодатель признает использование цифровых технологий квалифицирующим признаком задним числом, это может означать придание закону обратной силы, ухудшающей положение лица. Более обоснованной видится позиция Е.А. Русскевича, требующая осторожного подхода к криминализации. Однако и она не решает проблему полностью: как быть с ситуациями, когда сам предмет преступления (например, криптовалюта) появился уже после совершения деяния?

Считаем, что решение указанной проблемы заключается в необходимости закрепить в постановлении Пленума Верховного Суда РФ от 24.06.2025 № 10 «О практике применения судами положений ст. 10 УК РФ об обратной силе уголовного закона» правило, согласно которому при решении вопроса об обратной силе уголовного закона применительно к цифровым объектам следует исходить из их экономико-правовой сущности. Если цифровой актив выполняет функции, аналогичные традиционному предмету преступления (имущество, деньги), то применение закона должно определяться по правилам, установленным для соответствующих традиционных объектов.

Вторая проблема касается ситуаций, когда вред причиняется автономными цифровыми системами, а вопрос об ответственности человека возникает спустя значительное время после внедрения таких систем. Э.Л. Сидоренко подчеркивает, что традиционные конструкции вины и соучастия, сформированные для правовой реальности прошлого, оказываются неприменимыми в архитектуре распределенных реестров и автоматизированных систем. Автор справедливо задается вопросом: «Кому вменять ответственность в системе, где решение принимает автономный алгоритм, а смарт-контракт исполняет себя сам?» [6].

В доктрине высказываются различные мнения, например, И.Р. Бегишев предлагает рассматривать возможность признания искусственного интеллекта особым субъектом ответственности, вводя понятие «квазисубъектности» [1. С. 45]. Противоположная позиция (Ю.В. Грачева, С.В. Маликов, А.И. Чучаев) заключается в том, что предупреждение девиаций в цифровом мире уголовно-правовыми средствами должно осуществляться через традиционные институты, поскольку искусственный интеллект остается инструментом в руках человека [2. С. 201].

Концепция «квазисубъектности» искусственного интеллекта, безусловно, отражает технологические реалии, но вступает в противоречие с принципом вины, составляющим основу уголовной ответственности. Если система действовала автономно, а разработчик не мог предвидеть ее действия, применение уголовного закона, появившегося после причинения вреда, нарушало бы принцип «nullum crimen sine lege». В то же время отказ от ответственности вообще создает опасный пробел.

В качестве решения выявленной проблемы представляется необходимым законодательно закрепить правило о том, что при квалификации деяний с участием искусственного интеллекта обратная сила уголовного закона применяется только при доказанности двух обстоятельств: 1) наличие вины конкретного лица (разработчика, владельца, пользователя) в форме умысла или неосторожности; 2) возможность предвидения общественно опасных последствий на момент создания или внедрения системы. Целесообразно также введение института «уголовно-правового эксперимента», позволяющего ограниченно применять новые нормы к длящимся правоотношениям с участием искусственного интеллекта (далее – ИИ).

Третья проблема связана с появлением новых видов наказаний и иных мер уголовно-правового характера, реализуемых с использованием цифровых технологий. В.Ф. Лапшин и С.А. Хохрин обосновывают перспективность поиска альтернативы физической изоляции осужденного от общества в области лишения (ограничения) доступа к информационно-телекоммуникационным средствам связи, цифровым сервисам и иным цифровым ресурсам [3. С. 82].

В научной дискуссии сталкиваются две позиции. Сторонники внедрения «цифровых наказаний» (А.В. Шушеначев) указывают на их гуманистический потенциал и соответствие потребностям цифрового общества [10. С. 225]. Противники (А.В. Смирнов) предупреждают о рисках нарушения прав человека и недопустимости

применения таких мер к лицам, совершившим преступления до их законодательного закрепления [8. С. 31].

Дискуссия о «цифровых наказаниях» обнаруживает классическую коллизию между принципом гуманизма и принципом законности. С одной стороны, ограничение доступа к цифровым ресурсам может быть менее репрессивным, чем лишение свободы. С другой стороны, применение такой меры к лицу, совершившему преступление в эпоху, когда цифровые права не рассматривались как значимые ценности, нарушает правило об обратной силе

в его гуманистическом измерении.

Как нам думается, в решении указанной проблемы, будет оправданным применять дифференцированный подход: «цифровые наказания» могут применяться с обратной силой только в случаях, когда они улучшают положение осужденного по сравнению с ранее назначенным наказанием. При этом необходимо законодательно закрепить, что лишение или ограничение доступа к цифровым ресурсам допускается лишь при условии, что осужденный на момент совершения преступления обладал соответствующими цифровыми правами и осознавал их ценность.

Заключение. Проведенный анализ позволяет сделать вывод о том, что цифровая трансформация ставит перед теорией уголовного права и правоприменительной практикой сложные вопросы, связанные с действием обратной силы уголовного закона. Выделенные проблемные вопросы – определение момента появления цифровых объектов, квалификация деяний с участием ИИ и применение «цифровых наказаний» – требуют не точечных изменений, а системного переосмысления подходов к действию уголовного закона во времени.

Основным направлением решения выявленных проблем должно стать сочетание традиционных принципов уголовного права (законность, вина, справедливость) с новыми реалиями цифрового общества. Необходима выработка единых подходов к пониманию «цифрового предмета преступления», «цифровой вины» и «цифрового наказания» в контексте действия закона во времени. Только такой комплексный подход позволит обеспечить как эффективное противодействие киберпреступности, так и незыблемость фундаментальных прав и свобод человека в цифровую эпоху.

Список литературы

1. Бегишев И.Р. Уголовно-правовая охрана общественных отношений, связанных с робототехникой. – М.: Проспект, 2022. – 160 с.

2. Грачева, Ю. В. Предупреждение девиаций в цифровом мире уголовно-правовыми средствами / Ю. В. Грачева, С. В. Маликов, А. И. Чучаев // Право. Журнал Высшей школы экономики. – 2020. – № 1. – С. 189-211.

3. Лапшин В.Ф., Хохрин С.А. Альтернативы лишению свободы в условиях цифровой трансформации общества: эмпирическое исследование // Вестник ОмГУ. Серия. Право. – 2025. – №2. – С. 80-88.

4. Русскевич Е.А., Дмитренко А.П., Кадников Н.Г. Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации // Вестник СПбГУ. Серия 14. Право. – 2022. – №3. – С. 585-598.

5. Русскевич, Е. А. Цифровизация уголовного законодательства: непростые последствия простых решений // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2025. – № 5(129). – С. 26-33.

6. Сидоренко Э.Л. Алгоритмы и предупреждение проступка: о цифровизации уголовного права. URL: https://rapsinews.ru/White_Internet_news/20260212/311593486.html

7. Сидоренко Э.Л. Сидоренко призвала адаптировать уголовный процесс к цифровым реалиям. URL: https://rapsinews.ru/digital_law_news/20251112/311326608.html

8. Смирнов А.В. Электронные доказательства, электронное доказывание, искусственный интеллект: что дальше? // Уголовное судопроизводство. – 2024. – № 1. – С. 24-31.

9. Сундурова О.Ф. Цифровизация и сетевизация: проблемы дифференциации уголовной ответственности // Вестник ВУиТ. 2020. №4 (97). – С. 132-140

10. Шушеначев, А. В. Цифровые технологии в уголовном процессе: проблемы и риски // Вестник Российской правовой академии. – 2024. – № 1. – С. 214-229.

О. В. Обернихина,
преподаватель кафедры уголовно-исполнительного права и
организации исполнения наказаний,
не связанных с изоляцией осужденных от общества
(Кузбасский институт ФСИН России)

Применение обратной силы уголовного закона к новым составам преступлений в условиях цифровизации: проблемы квалификации и пути решения

Аннотация. В статье исследуются проблемы применения ст. 10 Уголовного кодекса Российской Федерации к новым составам преступлений, возникающим в процессе цифровой трансформации общественных отношений. Автором выделены два ключевых проблемных вопроса: отсутствие четких критериев оценки нового цифрового закона как более мягкого или более строгого, а также определение возможности применения обратной силы к деяниям, совершенным до криминализации соответствующих цифровых составов. Проведен анализ мнений ведущих ученых, предложены варианты решений выявленных проблем, включающие разработку методики комплексной оценки закона и дифференцированный подход к применению ст. 10 УК РФ в зависимости от природы цифрового деяния.

Ключевые слова: обратная сила уголовного закона, ст. 10 УК РФ, цифровизация, новые составы преступлений, киберпреступность, дипфейк, метавселенные, криминализация, принцип законности

Application of the retroactive effect of criminal law to new types of crimes in the context of digitalization: problems of qualification and solutions

Abstract. The article examines the problems of applying Article 10 of the Criminal Code of the Russian Federation to new types of crimes arising in the process of digital transformation of social relations. The author identifies two key problematic issues: the lack of clear criteria for assessing a new digital law as more lenient or more severe, as well as determining the possibility of applying retroactive effect to acts committed before the criminalization of relevant digital offenses. The analysis of opinions of leading scientists is carried out, solutions to the identified problems are proposed, including the development of a methodology for comprehensive assessment of the law and a differentiated approach to the application of Article 10 of the Criminal Code of the Russian Federation depending on the nature of the digital act.

Keywords: retroactive effect of criminal law, Article 10 of the Criminal Code of the Russian Federation, digitalization, new types of crimes, cybercrime, deepfake, metaverses, criminalization, principle of legality

Введение. Цифровая трансформация, охватившая все сферы жизни современного общества, ставит перед уголовно-правовой наукой новые вопросы. Как нам видится, в современных реалиях особую сложность представляет проблема применения ст. 10 Уголовного кодекса Российской Федерации (далее – УК РФ) к новым составам преступлений, возникающим в цифровой среде. Как справедливо отмечает Е.А. Русскевич, в осмыслении проблемы противодействия цифровой преступности нельзя не учитывать то вполне очевидное обстоятельство, что сетевое пространство стало местом ежедневной социальной активности подавляющего большинства населения страны [5. С. 27]. При этом появление новых цифровых благ и отношений требует необходимого правового регулирования и охраны.

Исследуя проблемы применения обратной силы уголовного закона, нельзя не отметить, что преобразование уголовного и уголовно-исполнительного законодательства дает предпосылки для обращения осужденных в суд по вопросам приведения приговора в соответствие с положениями нового закона, который улучшает их положение [3. С. 13]. Однако в условиях цифровизации возникает вопрос: как определить, улучшает ли новый закон положение лица, если сам состав преступления является принципиально новым и не имевшим аналогов в предшествующем законодательстве? Настоящая статья посвящена выявлению проблемных аспектов применения ст. 10 УК РФ к новым цифровым составам преступлений и поиску путей их разрешения.

Основная часть. Первая и наиболее фундаментальная проблема связана с отсутствием четких критериев определения того, является ли новый уголовный закон, устанавливающий ответственность за деяния в цифровой сфере, более мягким или более строгим по сравнению с ранее действовавшим регулированием. Данная проблема усугубляется тем, что многие цифровые составы преступлений не имеют прямых аналогов в традиционном уголовном праве.

Е.А. Русскевич отмечает, что цифровой способ совершения преступления далеко не всегда свидетельствует об увеличении общественной опасности деяния. Дополнение уголовного закона указанием на совершение преступления с использованием сети Интернет должно компенсировать реально сложившийся разрыв в степени общественной опасности между традиционной формой осуществления преступного посягательства и его цифровым аналогом [5. С. 28]. Автор предупреждает об опасности неоправданной цифровой казуализации уголовного закона, которая приводит к нарушению сложившихся моделей законодательного определения отдельных преступлений, а равно вступает в противоречие с доктринальными положениями, характеризующими содержание и пределы объективной стороны конкретных составов преступлений [5. С. 26].

И.Р. Бегишев и В.В. Денисович, исследуя метавселенные в уголовно-правовом измерении, приходят к выводу о необходимости полностью пересмотреть структуру объектов уголовно-правовой охраны и специфику привлечения к уголовной

ответственности лиц, обладающих специальными познаниями в сфере разработки продуктов достижений цифровых технологий. По мнению авторов, необходимо внести соответствующие изменения в УК РФ, учитывающие специфику виртуальных миров. При этом подчеркивается, что в любой метавселенной возможно совершение преступления тогда, когда в ней свою деятельность осуществляет человек. Это аксиоматичный вывод, который соответствует понятию преступления, закрепленному в ст. 14 УК РФ [2. С. 40].

Считаем важным обратить внимание законодателя и правоприменителя на то, что существуют два способа улучшения положения лица: изменение общих условий ликвидации уголовно-правовых последствий судимости; улучшение фактических условий ликвидации правовых последствий судимости, что обусловлено изменениями в уголовно-правовой оценке конкретного совершенного лицом деяния, его преступности и наказуемости» [3. С. 14]. Эта классификация важна для понимания механизма действия обратной силы, однако требует адаптации к цифровым реалиям, где само деяние может быть принципиально новым.

И.С. Алихаджиева, анализируя проблему дипфейков, отмечает, что манипулятивный потенциал феномена дипфейк настолько разнообразен, что в качестве цели его использования как средства совершения преступления может быть что угодно [1. С. 168]. Автор предлагает систематизацию составов преступлений, средством совершения которых может быть технология цифрового клонирования внешности и голоса человека, включая преступления против жизни, половой неприкосновенности, конституционных прав, собственности, общественной безопасности и другие [1. С. 169]. При этом она доказывает нецелесообразность наделения квалифицирующим признаком отдельных составов преступлений и приводит аргументы в пользу формулирования универсального отягчающего обстоятельства с его дополнением в статье 63 УК РФ [1. С. 166].

Мы полностью разделяем позицию И.Р. Бегишева о необходимости системного пересмотра объектов уголовно-правовой охраны применительно к цифровым технологиям. Вместе с тем, как справедливо отмечает Е.А. Русскевич, на поверку также оказывается, что цифровизация мало что добавляет и без труда «укладывается» в содержание законодательных моделей подавляющего большинства составов преступлений. Кража не перестает быть тайным хищением чужого имущества, будучи совершенной посредством неправомерного доступа к банковскому мобильному приложению потерпевшего [5. С. 28]. Это наблюдение имеет ключевое значение для применения ст. 10 УК РФ: если цифровое деяние охватывается традиционным составом, вопрос об обратной силе решается по общим правилам. Если же возникает принципиально новый состав (например, неправомерные действия с использованием технологии подмены личности), требуется выработка специальных критериев.

Позиция И.С. Алихаджиевой о предпочтительности универсального отягчающего обстоятельства перед созданием «цифровых двойников» отдельных

составов заслуживает поддержки, поскольку позволяет избежать конкуренции норм и упрощает применение ст. 10 УК РФ. При изменении редакции ст. 63 УК РФ оценка нового закона как улучшающего или ухудшающего положение лица должна производиться с учетом влияния соответствующего изменения на квалификацию и наказуемость деяния.

В свете указанных проблем для их соответствующего разрешения предлагается разработать и законодательно закрепить методику комплексной оценки нового цифрового закона, включающую: анализ изменений в санкциях статей (сравнение верхних и нижних пределов наказания); оценку влияния новых квалифицирующих признаков на категоризацию преступлений; учет изменений в правилах назначения наказания, рецидива, погашения судимости; сравнительный анализ санкций за аналогичные по степени общественной опасности традиционные преступления; оценку влияния изменений на правовой статус лиц, уже отбывающих наказание, с учетом различных способов улучшения положения лица.

Вторая проблема связана с установлением возможности применения ст. 10 УК РФ к деяниям, которые были совершены до цифровизации общества и криминализации соответствующих составов преступлений. Данная проблема имеет два аспекта: во-первых, возможность применения нового закона к деяниям, совершенным до его вступления в силу; во-вторых, возможность применения закона, улучшающего положение лица, к деяниям, которые на момент совершения не признавались преступными, но впоследствии были криминализированы с более мягкой санкцией по сравнению с аналогичными традиционными составами.

И.Р. Бегишев и В.В. Денисович указывают на то, что вопрос защиты персональных данных встает особенно остро в связи с ростом их оцифрованного объема по мере погружения в метавселенные. Роскомнадзор, а также иные правоохранительные органы высказывают справедливые опасения о возможном искажения привычных этических норм через понимание, что такое аватар человека и правовая реальность [2. С. 41]. Это наблюдение важно для понимания того, что многие цифровые деяния совершаются в условиях правовой неопределенности, когда ни законодатель, ни правоприменитель, ни сами граждане до конца не осознают их общественную опасность.

Е.А. Русскевич обращает внимание на то, что отставание социального контроля от технологии и тех качественных изменений, которые она привносит как в общественно полезные, так и во вредоносные формы поведения человека, имеет естественные причины и в истории наблюдалось не единожды [5. С. 27]. Однако это отставание порождает ситуацию, требующую специального правового регулирования: лицо, совершившее деяние с использованием новых цифровых технологий до их криминализации, не могло в полной мере осознавать общественную опасность своего поведения, что должно учитываться при решении вопроса об обратной силе.

Отметим, что на практике возникают ситуации, требующие законодательного урегулирования применения ст. 10 УК РФ, когда наказание осужденным либо полностью отбыто, либо лицо освобождено от его отбывания и возможность отмены освобождения себя исчерпала, судимость же не погашена и не снята [3. С. 14]. В цифровом контексте эта проблема усугубляется сложностью определения момента совершения преступления и длительностью существования цифровых последствий.

А.В. Серебренникова, проводя сравнительно-правовой анализ, отмечает многообразие подходов законодателей зарубежных государств к определению критериев криминализации, объектов и способов совершения преступлений в сфере цифровых технологий [6. С. 3]. Это свидетельствует об отсутствии универсальных решений и необходимости выработки собственных подходов с учетом национальной правовой традиции и международного опыта.

Е.В. Рогова подчеркивает, что цифровые технологии создают новые риски, такие как «киберхищения», «кибербуллинг», нарушение авторских прав, «сталкинг», распространение заведомо ложной информации, запрещенной информации, воздействие на общественное сознание и другие» [4. С. 123]. При этом она отмечает тенденцию включения признака использования информационно-телекоммуникационных сетей в качестве квалифицирующего в различные составы преступлений, что является достаточно обоснованным шагом с учетом высокого уровня информатизации общественных отношений [4. С. 124].

Соглашаясь с позицией И.Р. Бегишева о необходимости специального регулирования цифровых пространств, следует отметить, что применение обратной силы к деяниям, совершенным до криминализации, должно быть исключено в силу принципа «нет преступления без указания на то в законе». Однако, как справедливо отмечает Е.А. Русскевич, фиксируемое отставание права в условиях цифровизации само по себе не может выступать поводом для утверждения о глубоком кризисе и необходимости новых, соответствующих Индустрии 4.0 социальных регуляторов [5. С. 28]. Это означает, что традиционные принципы уголовного права сохраняют свое значение и в цифровую эпоху.

Кроме того, мы полагаем, что в обязательном порядке следует учитывать различные способы улучшения положения лица, причем это обстоятельство приобретает особое значение в цифровом контексте. Например, изменение категории преступления вследствие признания цифрового способа совершения деяния квалифицирующим признаком может влиять на сроки погашения судимости, что требует отдельной оценки при применении ст. 10 УК РФ.

В контексте сказанного предлагается законодательно закрепить следующие правила:

1. деяния, совершенные с использованием цифровых технологий до введения соответствующих составов преступлений, не подлежат уголовной ответственности, за

исключением случаев, когда они охватываются традиционными составами (например, кража, мошенничество, клевета);

2. при оценке возможности обратной силы нового цифрового закона необходимо учитывать, улучшает ли он положение лиц, совершивших аналогичные деяния до его принятия, в части смягчения наказания, исключения квалифицирующих признаков, изменения категории преступления или сокращения сроков погашения судимости;

3. для длящихся и продолжаемых преступлений в цифровой среде момент их окончания должен определяться по правилам, выработанным судебной практикой для традиционных преступлений;

4. при введении новых составов преступлений в цифровой сфере целесообразно сопровождать их специальными оговорками о действии во времени, аналогичными тем, что предусмотрены для универсального отягчающего обстоятельства, предложенного И.С. Алихаджиевой.

Заключение. Проведенный анализ позволяет сделать вывод о том, что применение ст. 10 УК РФ к новым составам преступлений, связанным с цифровизацией, порождает сложные теоретические и практические проблемы. Выделенные проблемные вопросы – отсутствие критериев оценки нового цифрового закона как более мягкого или более строгого, а также определение возможности применения обратной силы к деяниям, совершенным до криминализации цифровых составов – требуют системного переосмысления подходов к действию уголовного закона во времени.

Основным направлением решения выявленных проблем должно стать сочетание традиционных принципов уголовного права (законность, вина, справедливость) с новыми реалиями цифрового общества. Особого внимания заслуживает позиция И.Р. Бегишева о необходимости пересмотра структуры объектов уголовно-правовой охраны, с которой мы полностью солидарны. Вместе с тем, как справедливо отмечает Е.А. Русскевич, важно избегать неоправданной цифровой казуализации, создающей «цифровых двойников» традиционных составов. Важное значение имеет и позиция относительно необходимости учета различных способов улучшения положения лица, современную правоприменительную практику применения норм об обратной силе уголовного закона следует адаптировать к цифровым реалиям, при этом предложения И.С. Алихаджиевой о систематизации цифровых составов и универсальном отягчающем обстоятельстве могут служить основой для законодательных решений.

Разработанная методика комплексной оценки нового цифрового закона и дифференцированный подход к применению ст. 10 УК РФ позволят обеспечить как соблюдение принципа законности, так и учет особенностей цифровых преступлений при решении вопросов об обратной силе уголовного закона.

Список литературы

1. Алихаджиева И.С. Перспективы установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности (законопроект № 718538-8) // Известия Юго-Западного государственного университета. Серия: История и право. – 2025. – Т. 15, № 2. – С. 154-171.

2. Бегишев И.Р. Метавселенные в уголовно-правовом измерении / И.Р. Бегишев, В.В. Денисович // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции: в 6 т., Казань, 22 сентября 2023 года. – Казань: Познание, 2023. – С. 40-44.

3. Обернихина О.В. Действие обратной силы уголовного закона при снятии или погашении судимости // Актуальные вопросы борьбы с преступлениями. – 2014. – № 1. – С. 13-16.

4. Рогова Е.В. Дифференциация уголовной ответственности в современных условиях развития цифровых технологий // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: Материалы XXVIII международной научно-практической конференции. В 2-х частях, Красноярск, 03-04 апреля 2025 года. – Красноярск: Сибирский юридический институт МВД РФ, 2025. – С. 123-125.

5. Русскевич Е.А. Цифровизация уголовного законодательства: непростые последствия простых решений // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2025. – № 5(129). – С. 26-33.

6. Серебренникова А.В. Преступления в сфере цифровых технологий в законодательстве России и зарубежных стран: постановка проблемы // Кризисы мировой науки и техники: парадигмы дальнейшего развития: Материалы I Международной научно-практической конференции, Ростов-на-Дону, 20 апреля 2020 года. – Ростов-на-Дону: Южный университет (ИУБиП), 2020. – С. 62-67.

УДК 343.82

А. В. Павлова,
судья,
Новочебоксарский городской суд Чувашской Республики,
аспирант,
Чувашский государственный университет
имени И. Н. Ульянова,
Е. В. Нечаева,
кандидат юридических наук, доцент
Чувашский государственный университет
имени И.Н. Ульянова;
Казанский инновационный университет
имени В.Г. Тимирясова

Вопросы правоприменительной практики по замене назначенного судом уголовного наказания на принудительные работы в условиях цифровизации

Аннотация. На основании изучения материалов судебной практики Чувашской Республики анализируются проблемы, возникающие при замене назначенного судом уголовного наказания на принудительные работы, как на стадии назначения наказания, так и на стадии исполнения приговора. Рассматриваются возможности использования цифровых инструментов на стадии замены наказания другим видом.

Ключевые слова: принудительные работы, замена уголовного наказания, цифровое правосудие

A.V. Pavlova,
judge of the Novocheboksarsk City Court, Chuvash Republic,
graduate student of the Chuvash State University named after I. N. Ulyanov,
E.V. Nechaeva,
Law candidte, Associate professor
Chuvash State University named after I.N. Ulyanov;
Kazan Innovative University named after V.G. Timiryasov

Issues of law enforcement practice on substitution of criminal punishment appointed by the court with forced labor in the conditions of digitalization

Abstract. Based on the study of the materials of judicial practice of the Chuvash Republic, the problems arising when substitution of a criminal punishment imposed by the court with forced labor are analyzed, both at the stage of sentencing and at the stage of execution of the sentence. The possibilities of using digital tools at the stage of replacing punishment with another type are considered.

Key words: forced labor, substitution of criminal punishment, digital justice

Введение. На протяжении продолжительного времени в российской уголовно-правовой науке обсуждаются те или иные новеллы уголовного закона, направленные на либерализацию уголовно-правовой ответственности и наказания.

До недавнего времени велись ожесточенные споры вокруг целесообразности существования в системе наказаний, установленной в ст. 44 УК РФ, такого нового вида наказания как принудительные работы [6, С.45-49; 9, С.210-215]. Однако в последнее время наблюдается перенос вектора дискуссий от темы о сущности наказания в виде принудительных работ и их места в системе уголовных наказаний, к вопросу об их целесообразности и эффективности в случаях замены наказания.

По данным Судебного департамента при Верховном суде РФ за 2023 г. было вынесено 17 333 приговора к наказанию в виде принудительных работ. По сравнению с 2022 г. данный показатель вырос более чем в 5 раз. (3566 приговора) [8, С. 74], что свидетельствует об их востребованности и положительных тенденциях развития. Кроме того, применение наказания в виде принудительных работ не только как альтернативы лишению свободы, но и на стадии исполнения приговора в рамках замены наказания, содержит огромный потенциал для реализации цели исправления и пробации, что и обусловливает к ним особый интерес.

Основная часть. В иерархии перечня видов наказаний с точки зрения тяжести и порядка их применения принудительные работы, безусловно, являются примером смягчения репрессивности уголовного законодательства.

Введенные Федеральным законом от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [1] принудительные работы вызывают споры ученых-теоретиков, не до конца понятые обычными гражданами.

Правоприменительная реальность свидетельствует о том, что принудительные работы достаточно крепко укореняются как в целом в уголовно-правовой системе на стадии назначения наказания, так и на стадии исполнения приговора при замене назначенного судом наказания, как в сторону его смягчения, так и ужесточения.

Заложенный законодателем в указанный вид наказания правовой смысл свидетельствуют о том, что принудительные работы служат более ощутимому достижению закрепленных в п. 2 ст. 43 УК РФ целей наказания: восстановлению социальной справедливости, а также исправлению осужденного и предупреждению совершения новых преступлений.

С нашей точки зрения эффективное исполнение наказания происходит через труд, соединенный неразрывными связями осужденного с семьей, с обществом, что само по себе уже отвечает потребностям социального государства, основам общественных устоев, способствует развитию российского общества в позитивном русле.

В романо-германской (континентальной) правовой системе уголовного и уголовного - процессуального права отсутствует аналог принудительных работ. Так, например, в Уголовном уложении Федеративной Республики Германия (сокращенно - УУ ФРГ) - Strafgesetzbuch (StGB) содержится очень лаконичный перечень уголовных наказаний, где в качестве основных указываются: лишение свободы (§ 38- 39), назначаемый как самостоятельно, так и наряду с лишением свободы денежный штраф (§ 40-43); в качестве дополнительного: запрет управления транспортным средством (§44); в качестве дополнительного последствия: утрата пригодности занимать определенные должности, права быть избранным и права голоса (§ 45) [2].

Очевидно, принудительные работы являются прогрессивной новеллой российского уголовного права, самобытным явлением в нашей правовой системе, претендующим на повсеместную поддержку.

Вряд ли среднестатистический житель нашей страны сможет назвать существенные отличия между такими видами уголовных наказаний, как исправительные работы, обязательные работы и принудительные работы.

На начальном этапе введения этого вида наказания очевидны были сомнения и скептицизм, которые демонстрировались как правоприменителями, так и научным сообществом, обсуждая перспективы развития этого вида уголовного наказания.

На сегодняшний день ситуация представляется предельно ясной и понятной – принудительным работам предопределено получить широкое применение, об этом свидетельствуют все предпринимаемые государством меры.

Достаточно привести следующие факты и поделиться следующими профессиональными наблюдениями.

Уголовно-правовая политика в сфере регулирования применения принудительных работ начала ускоренно изменяться с 2018 года, когда Постановлением Пленума Верховного Суда РФ от 18.12.2018 № 43 (далее – Постановление № 43) [3] были внесены изменения в постановления Пленума Верховного Суда Российской Федерации от 20 декабря 2011 года № 21 «О практике применения судами законодательства об исполнении приговора» (далее – Постановление № 21) [4] и от 22 декабря 2015 года № 58 «О практике назначения судами Российской Федерации уголовного наказания» (далее – Постановление № 58) [5]. Постановлением № 43 были внесены дополнительно пункты 22.1-22.6 в Постановление № 58, регулирующие принудительные работы.

В дальнейшем начали создаваться изолированные участки, функционирующие как исправительный центр (далее – УФИЦ).

В настоящее время в Чувашской Республике функционирует 7 УФИЦ, при этом работа по созданию совершенствованию деятельности исправительных центров и УФИЦ в Чувашской Республике, как и во всех субъектах Российской Федерации, продолжается.

Таким образом, теоретическая и практическая базы для назначения принудительных работ государством в достаточной мере созданы.

Следует напомнить, что принудительные работы как вид наказания применяются на стадии вынесения судебного приговора и на стадии исполнения приговора при замене назначенного судом наказания на иное наказание.

Рассматривая первый вариант, до недавнего времени общепринятой формулировкой многих судебных приговоров была следующая фраза: «оснований для замены наказания в виде лишения свободы принудительными работами в порядке, установленном статьей 53.1 Уголовного кодекса Российской Федерации, не имеется».

Однако судебная практика последнего времени разворачивается в другую сторону. Количественные показатели о замене наказания на принудительные работы, как на стадии назначения, так и на стадии исполнения приговора, отдельно не выделяются в статистике Судебного департамента, однако, как показывают некоторые научные исследования [7, С.43-49] и личный практический опыт работы, цифры достаточно информативны. По данным только одного Новочебоксарского городского суда в 2023 году из всех поступивших материалов о замене наказания около 50% было удовлетворено.

Стала весьма распространенной становится ситуация, когда в судебных приговорах встречаются следующие выводы: «учитывая то, что подсудимый вину признал, согласился с обвинением в полном объеме, раскаялся в содеянном, характеризуется удовлетворительно, совершил преступление небольшой тяжести, подсудимый является трудоспособным, инвалидности не имеет, суд приходит к выводу, что для исправления подсудимого будет правильным применить положения ст. 53.1 УК РФ, то есть заменить лишение свободы принудительными работами».

При назначении принудительных работ у судов возникает законом предписанная необходимость в разрешении следующих уголовно-процессуальных вопросов:

– если подсудимый содержался под стражей, то произвести зачет срока содержания под стражей в отбытый срок принудительных работ из расчета один день содержания под стражей за два дня принудительных работ в силу положений п.3 ст. 72 УК РФ;

– в резолютивной части обвинительного приговора первоочередно назначить наказание в виде лишения свободы и вторым шагом в соответствии с положениями п.2 ст. 53.1 УК РФ заменить лишение свободы принудительными работами с указанием срока (в соответствии с п.4 ст. 53.1 УК РФ) и размера удержания заработка в доход государства (в соответствии с п.5 ст. 53.1 УК РФ);

– обязать подсудимого самостоятельно следовать к месту отбывания наказания за счет государства в соответствии с предписанием, заданным территориальным органом уголовно-исполнительной системы по месту жительства осужденного, в порядке, предусмотренном ч. 1 и ч. 2 ст. 60.2 УИК РФ;

– разъяснить осужденному, что в случае уклонения от получения предписания территориального органа уголовно-исполнительной системы (в том числе в случае неявки за получением предписания) или неприбытия к месту отбывания наказания в установленный в предписании срок осужденный объявляется в розыск и подлежит задержанию в срок до 48 часов, данный срок может быть продлен судом до 30 суток, после задержания осужденного к принудительным работам суд в соответствии со ст. 397 УПК РФ принимает решение о заключении осужденного под стражу и замене принудительных работ лишением свободы.

Если рассматривать второй вариант, то на стадии замены назначенного ранее судом уголовного наказания принудительные работы также начали широко применяться судами.

Следует отметить, что при замене наказания в случае злостного уклонения от его отбывания в порядке исполнения приговора, предусмотренном п. 2 ст. 397 УПК РФ, штраф, обязательные работы, исправительные работы, ограничение свободы заменяются принудительными работами без предварительной замены лишением свободы.

Принудительные работы также назначаются судом при замене неотбытой части наказания в виде лишения свободы.

Из общего анализа изученных нами судебных постановлений следует, что, как правило, зачастую осужденными не исполняются обязательные работы. Причины неисполнения формулируется чаще всего следующим образом: употреблял спиртные напитки, забыл, уехал на заработки и т.д. В случае частичного отбытия обязательных работ суды склонны заменять обязательные работы на принудительные работы, при этом указывается об удержании определенного процента из заработной платы в доход государства с отбыванием наказания в местах, определяемым учреждениями и органами уголовно-исполнительной системы, причем к месту отбывания наказания осужденному надлежит следовать самостоятельно за счет государства в соответствии с предписанием, выданным ему в порядке, предусмотренном частями 1 и 2 статьи 60.2 УИК РФ.

Суды при этом учитывают фактические обстоятельства преступления, за которое гражданин осужден, личность осужденного, и приходят к выводу о возможности исправления осужденного без реального отбывания им наказания в местах лишения свободы и заменяют осужденному неотбытое наказание принудительными работами.

Часто возникают ситуации, когда осужденный изначально не приступает к исполнению наказания в виде обязательных работ, открыто уклоняется от их исполнения, явно демонстрируя свое неуважение к вынесенному судебному акту, и становится очевидным, что наказание не будет отбыто. В таких случаях суды прибегают к крайней мере: заменяют обязательные работы сразу на лишение свободы, из расчета один день лишения свободы за восемь часов неотбытых обязательных работ.

Изученные нами судебные решения демонстрируют, что чаще всего на принудительные работы заменяются обязательные работы, но и назначенное судом лишение свободы может быть заменено на принудительные работы на стадии исполнения приговора в порядке замены неотбытой части наказания более мягким видом наказания в соответствии со ст. 80 УК РФ.

В судебной практике реже случаются прецеденты, когда неотбытая часть наказания заменяется более мягким видом наказания. Осужденные в своих ходатайствах о замене лишения свободы более мягким видом наказания, как правило, ссылаются на то, что они трудоустроены, принимают активное участие в воспитательных мероприятиях, вину признают, в содеянном раскаиваются, полностью или частично возместили причиненный преступлением ущерб. При разрешении ходатайства судом важными для анализа выступают следующие факторы: трудоустроен ли осужденный, как относится к труду, обучался ли он в учебных заведениях при исправительном учреждении, подвергался ли взысканиям за нарушения установленного порядка отбывания наказания, сняты и погашены ли взыскания, посещает ли мероприятия воспитательного характера, имеет ли поощрения, какие имеются особенности характера, как ведет себя в общении с представителями администрации учреждения, как относится к поручениям администрации учреждения, поведение и взаимоотношения в коллективе, с осужденными какой направленности (положительной или отрицательной) поддерживает связи, поддерживает ли отношения с родными и близкими, должником по каким исполнительным листам является, признает ли вину и т.д. Все эти определяющие моменты находят свое отражение в выдаваемой осужденному характеристике администрацией исправительного учреждения. Суды на основании анализа всех представленных доводов могут прийти к выводу о недостаточности изложенных осужденным обстоятельств для применения к осужденному положений статьи 80 УК РФ, поскольку суды не приходят к убеждению, что осужденный исправился и не нуждается в полном отбывании назначенного судом вида наказания, в связи с чем, в удовлетворении ходатайства осужденному может быть отказано.

Тем не менее, имеются многочисленные примеры в судебной практике, когда лицу, осужденному за совершение преступления, суд заменяет неотбытую часть наказания более мягким видом наказания, что, безусловно, способствует мотивации осужденного на дальнейшее законопослушного поведение.

Бесспорно, на ниве более широкого назначения принудительных работ на стадии исполнения приговора в порядке замены назначенного судом наказания, как в сторону ужесточения наказания, так и в сторону смягчения наказания, будут возникать новые практические вызовы, требующие внесения изменений в действующую законодательную базу, и новых разъяснений в Постановлениях Пленума Верховного Суда Российской Федерации и Обзорах судебной практики.

В настоящее время мы наблюдаем, что рассматриваемый вид уголовного наказания широко внедрился в практику и динамично развивается.

Сохранению положительных тенденций развития указанного института уголовного и уголовно-исполнительного права может способствовать применение инструментов технического прогресса, в том числе путем внедрения информационных технологий.

В последнее годы осуществляется планомерное внедрение в судебную систему информационных технологий. Важно, чтобы эти технологии оставались на уровне помощника в процессе осуществления правосудия, а не стали замещающим судью инструментами. С нашей точки зрения, цифровые технологии должны оставаться на уровне вспомогательных и не вмешиваться в самостоятельную процессуальную деятельность суда. Нарушение этой грани ведет к угрозе полной автоматизации вынесения судебных актов, что является, по-нашему мнению, недопустимым. Максимально возможным вмешательством информационных технологий является составление проекта судебного акта, при этом автором окончательного варианта судебного акта должен оставаться человек - судья, а не искусственный элемент - судья. На стадии исполнения судебного приговора при замене назначенного судом наказания допустимо использование некоторых информационных технологий для проведения, например, комплексного психолого-социального анкетирования осужденного, претендующего на замену неотбытой части назначенного судом наказания на иное наказание. Вопросы должны способствовать выявлению истинных намерений осужденного, мотивов его поведения, результаты могут быть обработаны цифровыми инструментами, путем исключения человеческого фактора, результаты этого анкетирования должны носить рекомендательный характер для суда и окончательное решение должно приниматься только судьей.

Заключение. Общая тенденция правоприменительной практики по замене назначенного судом уголовного наказания на принудительные работы в условиях цифровизации такова, что сегодня принудительные работы становятся все более популярным и действенным видом наказания, альтернативным лишению свободы, а широкое применение этого вида наказания является важным шагом на пути гуманизации уголовных наказаний, что не исключает применение цифровых технологий при рассмотрении вопросов замены наказаний на стадии исполнения приговора. Кроме того, применение наказания в виде принудительных работ не только как альтернативы лишению свободы, но и на стадии исполнения приговора в рамках замены наказания, содержит огромный потенциал для реализации цели исправления и пробации.

Список литературы

1. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федеральный закон от

07.12.2011 № 420-ФЗ // СПС «КонсультантПлюс» [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_122864/ (дата обращения: 05.09.2025).

2. Уголовное уложение Федеративной Республики Германия- Strafgesetzbuch (StGB). [Электронный ресурс]. URL.: https://www.uni-potsdam.de/fileadmin/projects/ls-hellmann/Forschungsstelle_Russisches_Recht/Neuauflage_der_kommentierten_StGB-%C3%9Cbersetzung_von_Pavel_Golovnenkov.pdf (дата обращения: 05.09.2025).

3. О внесении изменений в постановления Пленума Верховного Суда Российской Федерации от 20 декабря 2011 года № 21 «О практике применения судами законодательства об исполнении приговора» и от 22 декабря 2015 года № 58 «О практике назначения судами Российской Федерации уголовного наказания» : Постановление Пленума Верховного Суда РФ от 18.12.2018 № 43. // СПС «КонсультантПлюс» [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_313822/ (дата обращения: 05.09.2025).

4. О практике применения судами законодательства об исполнении приговора: постановление Пленума Верховного Суда Российской Федерации от 20 декабря 2011 года № 21 // СПС «КонсультантПлюс» [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_123850/ (дата обращения: 05.09.2025).

5. О практике назначения судами Российской Федерации уголовного наказания: Постановление Пленума Верховного Суда РФ от 22.12.2015 N 58 (ред. от 18.12.2018) // СПС «КонсультантПлюс» [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_190932/ (дата обращения: 05.09.2025).

6. Нечаева Е. В. Перспективы трансформации наказания в виде принудительных работ // Уголовно-исполнительное право. 2018. Т. 13(1-4), № 1. С. 45-49.

7. Селиверстов В.И. Принудительные работы: перспективы, пределы и риски развития // Пенитенциарная наука. 2024. №1 (65) [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/prinuditelnye-raboty-perspektivy-predely-i-riski-razvitiya (дата обращения: 05.09.2025).

8. Солоницын П.С. Замена наказания в виде принудительных работ на лишение свободы: вопросы теории и практики // Вестник Самарского юридического института. 2024. №3 (59) [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/zamena-nakazaniya-v-vide-prinuditelnyh-rabot-na-lishenie-svobody-voprosy-teorii-i-praktiki (дата обращения: 05.09.2025).

9. Тасаков С.В. Принудительные работы в системе наказаний уголовного законодательства Российской Федерации и проблемы их правоприменения // Актуальные проблемы экономики и права. 2015. № 3. С. 210-215.

УДК 343.2

Д. А. Писковатский,
ассистент кафедры,
Северо-Кавказский федеральный университет

Уголовно-правовые механизмы защиты информационного суверенитета Российской Федерации: проблемы квалификации преступлений и перспективы совершенствования законодательства

Аннотация. Статья посвящена исследованию основных направлений уголовно-правовой охраны информационного суверенитета Российской Федерации, рассматриваются теоретические основы и практические аспекты существующей нормативно-правовой базы, определяющей порядок противодействия преступлениям, связанным с нарушением информационной безопасности государства. Выделяются проблемы квалификации киберпреступлений и рассматриваются перспективы дальнейшего совершенствования законодательства в данной сфере.

Ключевые слова. Информационный суверенитет, уголовно-правовая охрана, киберпреступления, компьютерная информация, цифровизация законодательства

D.A. Piskovatsky,
Assistant of the Department of Criminal Law and Procedure,
North-Caucasus Federal University

Criminal and legal mechanisms of protecting the information sovereignty of the Russian Federation: problems of crime qualification and prospects for improving legislation

Abstract. The article is devoted to the study of the main directions of criminal and legal protection of the information sovereignty of the Russian Federation, examines the theoretical foundations and practical aspects of the existing legal framework that determines the procedure for countering crimes related to the violation of the state's information security. The article highlights the problems of qualifying cybercrimes and discusses the prospects for further improvement of legislation in this area.

Keywords. Information sovereignty, criminal law protection, cybercrimes, computer information, digitalization of legislation

Введение. Российская Федерация переживает период значительных изменений, затрагивающих все сферы жизни общества и государства. Эти изменения неизбежно отражаются и на законодательстве, особенно в области уголовного права. Уголовное право сегодня являются одними из наиболее развивающихся отраслей российской правовой системы, оно постоянно адаптируется к новым реалиям общества, экономическим условиям и международным стандартам. Эти факторы оказывают

существенное влияние на формирование новых тенденций развития уголовного права, требуя от ученых и практиков переосмысления традиционных подходов и поиска эффективных мер противодействия преступности в целом. Современный мир характеризуется расширением глобализационных процессов, стремительным развитием информационных технологий и появлением новых видов преступлений, посягающих на суверенитет Российской Федерации.

Основная часть. Суверенитет (от фр. souveraineté – верховенство власти) – это принцип международного права, согласно которому каждое государство обладает высшей властью на своей территории и имеет право самостоятельно решать внутренние дела, осуществлять внешние сношения и проводить независимую внутреннюю и внешнюю политику [4]. Исторически понятие суверенитета возникло в эпоху Средневековья и окончательно сформировалось в Новое время с развитием концепции Вестфальского мира (1648 г.). Сегодня суверенитет закреплен в Уставе ООН и других важнейших документах международного права [3]. В отличие от стран Европы Россия ни формально, ни юридически не отказывалась от собственного суверенитета и закрепила его как одну из основ конституционного строя (ст. 4 Конституции Российской Федерации). Развитие и усложнение общественных отношений отразились на содержательной трансформации российского суверенитета. В политической, экономической и правовой науке в последние годы активно идет дискуссия и об изменении содержания государственного суверенитета как ключевой для публично-правового и позитивно-правового регулирования категории. В документах различного уровня и юридической силы, в научных публикациях, в профессиональных сообществах стали употребляться (порой без научного обоснования в отличии от устоявшихся и всеми признанных терминов из конституционного права «государственный суверенитет», «народный суверенитет») такие термины как «информационный суверенитет», «цифровой суверенитет», «промышленный суверенитет», «технологический суверенитет», «продовольственный суверенитет», «экологический суверенитет», «научный суверенитет», «военный суверенитет» и др.

Информационный суверенитет – это способность государства самостоятельно определять политику в сфере информации, обеспечивать контроль над своими информационными ресурсами, защищать национальные интересы и безопасность от внешних информационных воздействий и угроз [1]. Информационный суверенитет является ключевым элементом национальной безопасности, поскольку информация играет центральную роль в современном мире. Без надежного контроля над собственными информационными ресурсами государство становится уязвимым перед внешними угрозами, которые выражены в кибератаках и взломах государственных информационных систем, распространение ложной или вредоносной информации, направленной на дестабилизацию общества, манипуляции общественным сознанием и политическими процессами посредством информационных атак и др.

Законодатель сегодня активно развивает нормативную базу, направленную на защиту своего информационного пространства и критической инфраструктуры. Это обусловлено растущими рисками и угрозой цифровизации, увеличивающими число потенциальных киберпреступлений. Рассмотрим наиболее значимые нормы Уголовного кодекса Российской Федерации (далее – УК РФ), направленные на охрану информационной сферы. Преступления против информационной безопасности и компьютерных данных закреплены в главе 28 УК РФ и именуется эта глава как преступления в сфере компьютерной информации.

Статья 274.1 УК РФ введена сравнительно недавно и направлена на борьбу с хищениями и использованием личной информации граждан. Умышленное получение данных без согласия владельца или субъекта влечет уголовное преследование вплоть до шести лет лишения свободы. Помимо статей 28 главы УК РФ существует ряд смежных положений УК РФ, обеспечивающих дополнительную защиту государственной тайны и объектов стратегического значения: статьи главы 29 («Преступления против основ конституционного строя и безопасности государства»), в частности, ст. 275–278 УК РФ регулируют государственные измену, шпионаж, диверсию и посягательство на территориальную целостность страны, затрагивая также сферу информационной безопасности, а также статья 283 УК РФ, относящаяся к разглашению государственной тайны, способствуя защите важной информации, составляющей государственную тайну [2].

Уголовно-правовая база Российской Федерации охватывает широкий спектр деяний, угрожающих информационной инфраструктуре и данным страны. Несмотря на существующие правовые инструменты, дальнейшее развитие норм требует учета новейших технологических достижений и динамично меняющихся условий глобальной сети Интернет. Квалификация преступлений, нарушающих информационный суверенитет государства, представляет собой сложную задачу, обусловленную рядом специфических проблем и правовых неопределенностей. Ниже рассмотрены основные трудности, возникающие при установлении состава преступления и привлечении виновных лиц к ответственности.

1. Трансграничный характер киберпреступлений. Большинство правонарушений, совершаемых в виртуальном пространстве, носят международный характер. Атака может осуществляться злоумышленниками, находящимися вне юрисдикции конкретного государства, что затрудняет установление конкретных исполнителей и сбор доказательств. Так, хакеры часто используют прокси-серверы, анонимайзеры и VPN-сервисы, скрывающие истинное местоположение преступников. Примером сложности привлечения к ответственности служит расследование случаев массового заражения компьютеров вирусами-шифровальщиками (ransomware). Хотя ущерб наносится гражданам различных государств, выявить инициаторов атак бывает крайне сложно.

2. Недостаточная определенность понятий и терминов. Законодательство зачастую не успевает за быстрым техническим прогрессом. Например, терминология в отношении вирусов и вредоносных программ устаревает, появляются новые методы воздействия, которые формально не охватываются действующими нормами закона. Это создает ситуации правовой неопределенности и сложности квалификации действий правонарушителей. Так, многие случаи внедрения вредоносного ПО квалифицировались бы как «хакерская атака», если бы соответствующее определение существовало в законе, однако судебная практика сталкивается с трудностями в применении общих формулировок законов.

3. Сложности установления субъектов преступления. При совершении преступлений в виртуальной среде злоумышленники могут действовать коллективно, используя сеть подставных аккаунтов, фейковых компаний и поддельных документов. Это значительно усложняет выявление реальных организаторов противоправных действий и фиксацию факта вины каждого из участников группы. Ярким примером является ситуация, когда одна группа занимается разработкой вируса, другая – осуществлением массовой рассылки зараженных писем, третья же получает средства от жертв вымогательской атаки. Привлечение всех членов преступной организации к ответственности осложняется сложностью доказывания взаимосвязей между ними.

Эффективная борьба с преступлениями против информационного суверенитета требует комплексного подхода, включающего как укрепление действующего законодательства, так и повышение качества правоохранительной практики. Ниже представлены конкретные предложения по улучшению российских нормативных актов и институтов, необходимых для успешной реализации целей информационной безопасности.

Актуализация уголовных норм: постоянное обновление уголовно-правовых норм в части определения новых типов преступлений, связанных с новыми технологиями и методами воздействия на информационную среду. Особое внимание уделить вопросам внесения изменений в главу 28 УК РФ («Преступления в сфере компьютерной информации»). Четкость юридических конструкций: установить четкую дефиницию ключевых понятий, используемых в нормах о преступлениях в сфере ИТ, таких как «компьютерная информация», «недостоверная информация», «распространение ложных сообщений». Расширение перечня квалифицирующих признаков: добавить новые обстоятельства, влияющие на квалификацию преступлений, таких как масштаб нанесенного ущерба, наличие специальной цели (дестабилизация общественной жизни, пропаганда экстремистских идей), принадлежность к группировке (организованная преступная деятельность в сети).

Заключение.

Таким образом, защита информационного суверенитета Российской Федерации приобретает особую значимость в условиях современной технологической реальности. Информационные ресурсы становятся объектом все большего количества угроз,

исходящих как изнутри страны, так и извне. Российской Федерации важно учитывать глобальные тенденции и адаптироваться к ним. Необходимость активного реформирования юридической базы и выстраивания надежных защитных барьеров продиктована требованием обеспечить устойчивое развитие и сохранение внутреннего порядка, гарантирующего свободу функционирования гражданского общества и экономики страны.

Список литературы

1. Ефремов А. А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. №1. URL: https://cyberleninka.ru/article/n/formirovanie-kontseptsii-informatsionnogo-suvereniteta-gosudarstva (дата обращения: 01.08.2025).

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 23.07.2025).URL: https://www.consultant.ru/document/cons_doc_LAW_ (дата обращения: 01.08.2025).

3. Устав Организации Объеденных Наций (полный текст) // Официальный сайт ООН [Электронный ресурс]. URL: https://www.un.org/ru/about-us/un-charter/full-text (дата обращения: 30.07.2025).

4. Холодная Е.В. Об информационном суверенитете // Вестник Университета имени О. Е. Кутафина. 2024. №10 (122). URL: https://cyberleninka.ru/article/n/ob-informatsionnom-suverenitete (дата обращения: 30.07.2025).

УДК 347.7

Г. В. Романова,
кандидат юридических наук,
Казанский институт (филиал) ВГУЮ (РПА Минюста России)

К вопросу о методике расследования преступлений в сфере компьютерной информации

Аннотация. В настоящей статье исследованы особенности методики расследования преступлений в сфере компьютерной информации. Дается понятие преступлений в сфере компьютерной информации, раскрывается характеристика состояния преступности в данном направлении. Особое внимание отводится отдельным элементам криминалистической характеристики: личности преступника, типичной обстановки, способам совершения преступного деяния. Изучается система следообразования. Проводится анализ особенностей производства следственных действий, наиболее характерных для рассматриваемой категории уголовных дел. Рассматриваются проблемные вопросы и предлагаются решения в связи с расследованием преступлений с использованием цифровой информации, использованию новых форм специальных знаний в данной сфере.

Ключевые слова: расследование преступлений, цифровая информация, криминалистическая методика, электронный носитель, информационный ресурс, расследование

G. V. Romanova,
Candidate of Law,
Associate Professor of the Department,
Kazan Institute (branch) of VSUJ (RPA of the Ministry of Justice of Russia)

On the methods of investigating computer crimes

Abstract. This article explores the features of the methodology for investigating crimes in the field of computer information. It defines the concept of crimes in the field of computer information and provides a description of the state of crime in this area. Special attention is given to individual elements of the forensic characteristics, such as the criminal's personality, the typical environment, and the methods used to commit a crime. The article also examines the system of trace formation. It analyzes the specific features of investigative actions that are most common in this category of criminal cases. The article addresses problematic issues and suggests solutions related to the investigation of crimes involving digital information and the use of new forms of specialized knowledge in this field.

Keywords: crimes, computer information, methodology, electronic media, and information resources, investigation.

Введение. В настоящее время информация, содержащаяся на компьютерном устройстве, стала важной частью многих сфер деятельности современного государства и общества, облегчая жизнь современному человеку. Одновременно внося и дискомфорт, позволяя преступникам совершать противоправные действия.

Методика расследования преступлений, совершаемых при помощи компьютерных устройств, способствует формированию знаний и выработке опыта борьбы с подобными деяниями.

Основная часть. Преступление рассматриваемой нами группы представляет собой виновное, общественно-опасное деяние, совершаемое при помощи современных технических компьютерных устройств, посредством воздействия на информационные ресурсы, содержащиеся в электронно-информационной, цифровой среде, не зависимо от способов и средств хранения, распространения и передачи.

Специфика компьютерных преступлений находит свое непосредственное отражение в выбираемых преступником способах совершения противоправных деяний. Например, подбор паролей, получение доступа к информации обманным путем, проникновение в компьютер с использованием своего служебного положения, заражения технического устройства вирусной программой и многие другие.

Построение оптимальной методики расследования преступлений в сфере компьютерной информации основывается на знании криминалистической характеристики указанных преступлений, таких как личностные качества преступника (при этом обращая особое внимание на уровень подготовки, амбициозность, замкнутость, стремление уйти от реальности, и т.д.), место и способы совершения преступного деяния, картина следообразования.

Особенность рассматриваемой нами группы преступлений часто проявляется в выборе сложных способов воздействия на используемый информационный ресурс, формируемый преступниками в виде оставленной дорожки следов противоправной деятельности. Например, файлы программного обеспечения; лог-файлы, журналы, отчеты операционной системы; сведения, полученные с сервера компьютерного устройства, с мессенджеров цифровых устройств, используемых преступниками для общения и связи между собой и т.д.

На наш взгляд, выбор методики расследования должен учитывать сложность технической комплектации компьютера, наличие защиты программных устройств, заранее установленных пользователем и способами взлома со стороны преступника, понимания личности современного преступника, отличающегося особой сообразительностью, подготовленностью, образованностью.

Часто совершаемые компьютерные преступления связаны с неправомерным доступом к компьютерной информации. Следователю необходимо проанализировать сам факт неправомерного вторжения злоумышленника в компьютер пользователя, получение доступа к информации, хранящейся в устройстве потерпевшего;

последствия совершенных действий (копирования информации, удаления или ее модификация); личность преступника (к примеру, служебное положение или корыстная заинтересованность). Доказывание факта неправомерности доступа к компьютерной информации возможно путем анализа внутренней документации потерпевшего, справочной информации, действий потерпевшего по защите его персональных данных, наличия установленных на компьютерном устройстве защитных программ, периодичность их обновления, а также возможность доступа посторонних лиц к паролям, сервисам защиты и к местам нахождения компьютерной техники. Корыстная заинтересованность, как правило, доказывается путем приобщения справок и выписок с банковского счета подозреваемого, подтверждающих получение дополнительного дохода с помощью совершенного преступления. Служебное положение подтверждается фактом наличия логина и пароля от справочной компьютерной системы в результате выполняемых лицом должностных обязанностей.

Виртуальность развития кибернетического пространства предусматривает возможность использование сразу нескольких компьютерных устройства для совершения преступления. В этом случае выбор методики расследования будет учитывать временной промежуток совершаемых злоумышленником действий, периодичность зловредных атак, продолжительность самого посягательства, наступления общественно опасных последствий.

Не следует исключать способность программного обеспечения осуществлять защиту компьютера: блокировать систему, запрещать доступ постороннему лицу или устройству. В этом случае анализируется система идентификации пользователей, имеющих доступ к компьютеру, проводится мониторинг действий пользователя, частота использования межсетевого экрана или брандмауэра для защиты от сетевых угроз.

Судебно-следственная практика позволяет проанализировать условия совершения преступления. Об этом свидетельствует статистика и опыт в борьбе с такими преступлениями. Только за первые три месяца 2025 года в России зафиксировано более 6 тыс. преступлений, связанных с информационными технологиями. Из них раскрыто только 1249 дел – это чуть больше 20% [3].

Работа следователя по подбору методики расследования преступлений рассматриваемой группы имеет определенные сложности. Во-первых, необходимость изучения программ и вирусов, способных существенно навредить компьютерному устройству в результате стремительного проникновения в систему. Во-вторых, анализируются последствия произошедшего противоправного события. В-третьих, оценивается реальная и виртуальная обстановка, в которой преступник намеревался или совершал преступление.

Большинство следов после совершения компьютерного преступления остаются на месте происшествия в результате поспешных, необдуманных спонтанных действий преступника.

Например, на игровой онлайн-платформе Roblox в 2025 году было зафиксировано 40 преступлений. Преступники выманивали у детей деньги, доступы к аккаунтам и к личной информации. Чаще всего преступления совершались под предлогом розыгрыша внутриигровой валюты.

Следственными органами была выявлена следующая схема работы преступников: несовершеннолетний общался в чате игрового устройства с куратором. Злоумышленник был хорошо подготовлен к подобному общению, психологически грамотен, обладал знаниями общения с несовершеннолетней аудиторией, понимал азартный настрой вовлекаемых лиц, уровень игровой зависимости. В результате противоправных действий преступники просили несовершеннолетнюю жертву сообщить им данные банковской карты, логины и пароли от нее (свои или данные карты родителей, опекунов или попечителей) [4].

Как нам представляется методика расследования изучаемой нами группы преступлений требует от следственных органов активных действий с применением комплекса знаний и умений.

Первоначальный этап расследования обусловлен следующими следственными ситуациями, классифицируемыми по субъекту выявления факта преступления:

– собственник или владелец компьютерной информации (потерпевший) обнаружил факт преступления, самостоятельно выявил, изобличил и задержал преступника;

– владелец информации установил факт преступного посягательства, но преступник не известен;

– преступление обнаружено правоохранительными органами.

Следственные ситуации в процессе выработки методики расследования позволяют вырабатывать основу для построения частных и общих криминалистических версий.

Порой неотложные следственные действия включают:

– осмотр места происшествия или отдельных предметов;

– выемку;

– допросы свидетелей, потерпевшего;

– и другие по метре необходимости.

В случаях, если подозреваемый установлен, то он задерживается, проводятся обыски по месту его нахождения, проживания, работы, подозреваемый допрашивается [2. С. 76].

Важными и одновременно проблемными становятся задачи, решаемые в результате следственных действий, а также сопутствующие их оперативно-розыскные мероприятия, такие как:

– выбор, изучение полученной информации о способе совершенного преступления, личности преступника, его профессиональном опыте;

– фиксация обстановки совершенного преступления, наличия установленных защитных механизмов и программ в компьютере;

– определение размера причиненного ущерба.

Методика расследования компьютерных преступлений требует профессионального взаимодействия следователя и специалиста при проведении следственных действий. Как, правило, осмотр, обыск, выемка происходят с участием специалиста. Консультация специалиста может потребоваться при подготовке следователя к допросу подозреваемого, обвиняемого, потерпевшего, а также при формировании вопросов эксперту [7. С. 22].

На первоначальном этапе расследования проводится осмотр места происшествия с целью выявления и фиксации информации, позволяющей установить и запечатлеть виртуальный след, оставленный преступником, познать его специфику. Если при проведении осмотра используются специальные поисковые технические устройства, то в протоколе следственного действия делается специальная отметка с указанием и описанием всех индивидуальных признаков используемых приборов (марка, тип, заводской номер, название и т.д.). Не менее важным стоит указать, что устройство применялось специалистом.

Работа с виртуальными следами требует особой внимательности со стороны следователя: обнаруженный след подлежит особой защите. Контакт подозреваемого с иными лицами должен быть исключен или минимизирован с целью сохранения оставленного следа на месте преступления, исключения его последующего уничтожения. Предметы, найденные в пределах территории обнаруженного следа, подлежат тщательному осмотру, анализу на предмет возможного использования преступником.

Практика подтверждает, что помощь потерпевшего, активное сотрудничество подозреваемого со следователем на первоначальном этапе расследования ускоряют процесс расследования. Потерпевший – владелец компьютерной системы, обнаруживает нарушение целостности и конфиденциальности данных, а также факт вторжения в индивидуальное компьютерное пространство (обстоятельства, признаки, потери данных пользователя), о которых незамедлительно сообщает в правоохранительные органы. При этом совершать противоправные действия с целью корыстного обогащения могут лица, работающие на потерпевшего. Например, гр. А. реализуя корыстные цели согласился за денежное вознаграждение передать третьим лицам сведения, составляющие коммерческую тайну: список абонентов компании, их персональные данные, информацию, связанную с обслуживанием в рамках заключенных договоров. Копирование персональных данных гр. А осуществил при помощи своего знакомого программиста гр. К., передав ему логин-пароль от своей учетной записи [6]. В другом случае, потерпевший – провайдер помогает пользователю, а в последующем и следственным органам, установить и подтвердить факт незаконного списания денежных средств с электронного банковского счета, предоставить

необходимые разъяснения по поводу процедуры и обстоятельств списания, сведений о подключенном и используемом при этом техническом компьютерном устройстве, а возможно и следах, которые мог оставить злоумышленник – не профессионал. Например, Отделением Фонда пенсионного и социального страхования РФ в течение года после смерти гражданки ежемесячно начислялась страховая пенсия по старости путем зачисления денежных средств на ее банковский счет. Родственница умершей, имея доступ к банковскому счету и банковской карте еще при жизни гражданки, скрыв факт ее смерти, зная о продолжающемся регулярном поступлении денежных средств на счет умершей, своевременно их похищала путем ввода известного ей пин-кода от мобильного приложения онлайн-банка и последующего перевода денег на свой электронный счет, в дальнейшем используя их по своему назначению и осознавая противоправность совершаемых действий [5].

Взаимодействие следователя с оперативниками, специалистами также положительно влияет на получение необходимой информации по делу. В рамках совместной работы на месте происшествия все общение между следователем и сотрудником оперативно-розыскного органа, а также специалистом происходят в устной форме. Устное общение включает в себя обмен информацией, совместное обсуждение деталей осматриваемого технического компьютерного устройства, помещения в котором оно находится, сопоставление и систематизацию полученных сведений. В этом случае устная форма общения считается наиболее благоразумной и уместной. Поручения следователя в устной форме также очевидны. Однако отсутствие законодательного закрепления требования выполнять устные поручения следователя иногда бывает формальным поводом для отказа в их последующем исполнении, что безусловно приобретает отрицательные последствия для процесса расследования.

Последующий этап расследования преступлений в сфере компьютерной информации предусматривает изучение полученной информации, особенно касаемой способа совершения преступления, объекте и предмете преступного посягательства, установление преступника (если все еще не известен), проверку общих версий.

Например, в отношении гр. С. было возбуждено уголовное дело, назначена компьютерно-техническая экспертиза, производство которой было поручено государственному учреждению. Эксперту были четко определены вопросы, интересующие следствие по поводу произошедшего события. Однако в последующем стало известно о том, что эксперт оказался сотрудником частной организации, деятельность которой была далека от запрашиваемых судом услуг. Эксперт также не владел теми навыками и знаниями, которые от него требовали, он практиковался в иных направлениях, что в последующем сказалось на достоверности полученных доказательств [1].

Таким образом, основное предназначение методики расследования преступлений в сфере компьютерных технологий состоит в обеспечении следователя и взаимодействующих с ним лиц научно-методическими знаниями о методах

раскрытия и расследования противоправных событий с использованием современной компьютерной техники в различных следственных ситуациях.

Список литературы

1. Апелляционное определение Судебной коллегии по уголовным делам Санкт-Петербургского городского суда от 20.04.2017 по делу № 22-2649/2017.

2. Криминалистика: конспект лекций: учебное пособие /В.П. Лавров, Р.Р. Рахматуллин, В.И. Романов, А.Н. Шалимов. М.: Проспект.2023.

3. Новости г. Казани и Татарстана. Газета ТатарИнформ. Новость за 23 мая 2025 года // www.tatar-inform.ru.

4. Новости. Газета Коммерсант. 21.03.2025. www.kommersant.ru.

5. Приговор Златоустовского городского суда Челябинской области от 22.01.2025 по делу № 1-76/2025.

6. Приговор Орджоникидзевского районного суда г. Екатеринбурга от 27.07.2017 № 1-405/2017, дело № 1-405/12.

7. Романова Г.В. Цифровые доказательства: понятие, особенности, проблемы использования в современном законодательстве и практике его применения. Учебное пособие. Казань: редакционно-издательский центр «Школа», 2023. 171 с.

УДК 343.131.5

А. А. Самохвалов,
аспирант,
Челябинский государственный университет

Электронный документ в досудебном производстве по уголовному делу: критический анализ на основе института обжалования

Аннотация. Целью исследования является выявление проблемных вопросов использования института обжалования при внедрении цифровых технологий в уголовно-процессуальное право. Исследование акцентирует внимание на наиболее вероятных способах дальнейшего использования цифровых технологий на стадии досудебного производства по уголовному делу. Дополнительно выявляются вопросы информационной безопасности и признания юридической силы ходатайств и жалоб в электронном виде. Проводятся параллели с наиболее развитой системой цифровизации англо-саксонского уголовно-процессуального права. В качестве вывода установлена необходимость постепенного развития процессуальных норм с целью развития внедрение информационных технологий в институт обжалования.

Ключевые слова: уголовно-процессуальное право, цифровые технологии, электронный документ, досудебное производство, ходатайство, жалоба, цифровизация

A. A. Samokhvalov,
Postgraduate student of the Department of Criminal Law Disciplines,
Chelyabinsk State University

Electronic document in pre-trial proceedings in a criminal case: critical analysis based on the institute of appeal

Abstract. The goal of the article is to identify problematic issues of the application of the institute of appeal when introducing digital technologies into criminal procedural law. The scientific article examines the most likely ways of further use of digital technologies at the stage of pre-trial proceedings in a criminal case. In addition, issues of information security and recognition of the legal force of applications and complaints in electronic form are considered. Parallels are drawn with the most developed system of digitalization of Anglo-Saxon criminal procedural law. As a conclusion, the need for a gradual development of procedural rules in order to develop the implementation of information technologies in the institute of appeal is established.

Keywords: criminal procedure law, digital technologies, electronic document, pre-trial proceedings, petition, complaint, digitalization

Введение. Планомерное развитие цифровых технологий и электронного документооборота в различных отраслях права является теоретической и практической новеллой, представляет собой трансформацию правовых отношений, проявляющуюся в повсеместном использовании цифровых технологий, в том числе и при расследовании уголовных дел.

Необходимо учесть, что внедрение цифровых технологий в уголовно-правовые и уголовно-процессуальные отношения находится в стадии формирования. Только в 2023 году Федеральным законом от 25.12.2023 № 672-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» была введена статья 474.2, регулирующая порядок использования электронных документов в ходе досудебного производства. Согласно данной статье использование электронных документов в ходе досудебного производства ограничивается технической возможностью органа дознания. В связи с чем, несмотря на законодательную регламентацию электронного документооборота в рамках досудебного производства.

При использовании в ходе досудебного производства электронного документооборота складывается особая специфика процессуальных отношений, отличающаяся от традиционных приемов и способов ведения досудебного производства как стороной обвинения, так и стороной защиты. Данная специфика складывается из особенностей производства по уголовным делам при использовании цифрового пространства: программным обеспечением, компьютерным оборудованием, сетевыми устройствами [11. С. 67].

В процессе регулирования возникающих правоотношений предстоит решить ряд научных и практических вопросов, затрагивающих теоретические и законодательные начала уголовно-процессуального права в части изменения устоявшихся правовых норм на новые стандарты и правила расследования уголовного дела.

А. М. Долгов считает, что направление в электронном виде ходатайств и жалоб в органы предварительного следствия и прокурору станет дополнительной необходимой гарантией защиты прав и свобод человека. Кроме того, цифровизация уголовного производства станет дополнительной гарантией защиты прав и свобод потерпевшего от преступления [3. С. 58].

В то же время другие ученые оценивают уровень цифровизации и информатизации уголовного процесса как соответствующий начальному этапу создания цифровых платформ правоохранительных органов и судебной системы [9. С. 173].

С точки зрения осуществления адвокатской деятельности по защите подозреваемого (обвиняемого) на стадии досудебного производства по уголовному делу, введение электронного документооборота может быть рассмотрено как наиболее удобный вариант осуществления защиты, сокращающий временные затраты. Однако в данном случае стоит учесть все правовые и технические особенности направления электронного документа, которые не могут быть учтены без детальной законодательной

регламентации адвокатской деятельности в цифровом пространстве, что особенно важно при направлении ходатайств и жалоб на действия (бездействие) должностных лиц на стадии досудебного производства по уголовному делу.

Учитывая высокую формализацию расследования уголовных дел, введение электронного документооборота в досудебное производство представляется целесообразным и необходимым. Возможность направления электронного документа в рамках досудебного производства по уголовному делу может ускорить передачу дела в суд, разгрузить органы следствия, повысить работоспособность и упростить порядок взаимодействия работников следственных органов, органов дознания.

Л. А. Шестакова отмечает высокий уровень цифровизации уголовного процесса в станах континентальной Европы, в которых подача электронных ходатайств и жалоб. В ходе анализа цифровизации уголовного судопроизводства было выявлено наличие взаимодействия государства и граждан посредством системы электронного документооборота, осуществление правового регулирования сбора электронной информации, носителей электронной информации и правового статуса электронной информации, использование видео-конференц связи, внедрение технологии «электронное уголовное дело» [12. С. 92-93].

Европейский и американский пути развития информатизации и цифровизации уголовного судопроизводства несомненно важны для развития уголовно-процессуального права Российской федерации в данной сфере. Определенно не все законодательные решения окажутся полезными для российского уголовного судопроизводства, но тем не менее, при интеграции информационных технологий в уголовный процесс следует учитывать европейский опыт и опыт США.

В части направления ходатайств и жалоб могут возникнуть дополнительные проблемы. Цифровизацию института обжалования необходимо проводить с учетом действующих положений.

В качестве основы вносимых в правовое регулирование института обжалования изменений следует принимать действую уголовно- процессуальную регламентацию института обжалования.

Институт обжалования регулируется главой 16 Уголовно-процессуального кодекса Российской федерации (далее – УПК РФ). Указанные в данной главе нормы направлены на осуществление основных принципов уголовного судопроизводства, таких как принцип законности и принцип состязательности уголовного процесса.

Глава 16 УПК дает защитнику возможность оказания квалифицированной юридической помощи подозреваемому-обвиняемому по уголовному делу путем направления ходатайств и жалоб на действия (бездействие) следственных органов и должностных лиц, осуществляющих досудебное производство по уголовному делу.

В свете изменений, вызванных всеобщей цифровизацией, которой подверглась и сфера уголовного правосудия, процедура подачи жалоб должна отвечать объективным

потребностям информационного общества и государства в развитии цифровизации и расширении сферы использования цифровых технологий [4. С. 210].

В данном случае встает актуальный вопрос дополнительной регламентации цифровизации обжалования в уголовном судопроизводстве. Если у адвоката, в силу своей профессиональной деятельности, зачастую имеется техническая возможность подачи жалобы в электронном виде то остается открытым вопрос наличия технической возможности у должностных лиц, в адрес которых направляется ходатайство и жалоба. Объективно, отсутствие специальных единых информационных систем взаимодействия между участниками уголовно-процессуальных отношений ставит под сомнение свободу обжалования в электронном виде.

Основная часть. УПК РФ содержит множество норм, регулирующих направление документов, имеющих значение для уголовного дела. Практически все действия участников досудебного производства должны быть зафиксированы в письменной форме. В настоящее время законодательством закрепляется письменная фиксация предварительного следствия по уголовному делу, тогда как электронный документооборот рассматривается как дополнительный способ формирования материалов уголовного дела.

Для систематического и результативного использования цифровых технологий с целью направления ходатайств и жалоб при защите адвокатом подозреваемого (обвиняемого) на стадии досудебного производства по уголовному делу, наличие, либо отсутствие технической возможности не является единственным возможным ограничением. Статьи 474.1, 474.2 УПК РФ включают в себя нормы об обязательном подписании таких документов электронной цифровой подписью с целью придания им юридической силы.

Придание юридической силы электронному документу является важнейшим вопросом использования электронного документооборота на стадии предварительного расследования. При использовании электронного документооборота необходимо обеспечить возможность проверки юридической силы документов, исключая несанкционированный доступ к электронным документам.

Разрешение вопроса проверки юридической силы документа является первоочередным в процессе повсеместного внедрения цифровых технологий в уголовно-процессуальное право.

Документ, подписанный электронной подписью может быть признан равнозначным документу на бумажном носителе, подписанному собственноручно при условии соблюдении ряда требований, установленных статьей 6 Федерального закона от 6 апреля 2011 г. № 63-ФЗ«Об электронной подписи». Кроме того, частью 1 вышеуказанной статьи указано, что информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с

законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Данная норма обуславливает презумпцию подлинности квалифицированной электронной цифровой подписи (усиленной квалифицированной электронной подписи), кроме того, использование данного вида цифровой подписи необходимо для направления электронных документов в досудебном производстве, в том числе при направлении ходатайств и жалоб.

Электронная цифровая подпись несомненно нуждается в защите от незаконного проникновения и копирования данных. Учитывая распространенность электронных цифровых подписей, современные меры защиты не дают гарантии от противоправных действий третьих лиц, не смотря на высокую степень надежности кодировки информации. Данный недостаток снижает преимущества электронной цифровой подписи [14. С. 3].

Данный факт обуславливает необходимость дополнительных проверок электронных документов в уголовном процессе и препятствует внедрению цифровых технологий в уголовное судопроизводство, в частности при использовании института обжалования.

При подаче ходатайства или жалобы в виде электронного документа необходимо предусмотреть дополнительные механизмы проверки подлинности электронного документа, так как неправомерно поданная жалоба может негативно повлиять на ход досудебного производства по уголовному делу. Необходимо законодательно закрепить примы и способы проверки подлинности электронного документа, направленного в рамках предварительного следствия. В настоящий момент данный вопрос недостаточно проработан, в связи с чем направление ходатайства или жалобы в виде электронного документа не может являться способом, гарантирующим защиту прав и свобод подозреваемого (обвиняемого) на стадии досудебного производства по уголовному делу.

Кроме вышеперечисленного следует упомянуть об издержках на изготовление электронной цифровой подписи, так как остается нерешенным вопрос об изготовлении электронной цифровой подписи для всех участников уголовного с целью упрощения их взаимодействия в рамках уголовного дела. В некоторых научных работах предлагается законодательное закрепление права на получение электронной подписи участниками судопроизводства на безвозмездной основе, опираясь на практику выдачи электронной подписи руководителям организаций и индивидуальным предпринимателям [10. С. 204].

Данная практика внедрения электронных технологий неплохо зарекомендовала себя в бизнесе и других отраслях права, но совершенно не подходит для досудебного

производства по уголовному делу при отсутствии электронного взаимодействия между сторонами обвинения и защиты.

Норма о получении электронной цифровой подписи всеми участниками уголовного судопроизводства неэффективна в отношении подозреваемого (обвиняемого) так как в отношении него судом может быть избрана мера пресечения в виде запрета определенных действий (пункт 5 части 6 статьи 105.1 УПК РФ) или заключения под стражу (статья 108 УПК РФ), в связи с чем подозреваемый (обвиняемый) может быть лишен возможности выхода в интернет при намерении направить ходатайство или жалобу.

Внедрение данных предложений в рамках информатизации уголовного процесса может быть целесообразно по отношению к адвокатам, с целью обеспечения дополнительной защиты прав и законных интересов доверителя посредствам использования института обжалования, но следует обратить внимание на то, что наличие электронной цифровой подписи у адвоката не расширяет возможности обеспечения защиты без системы электронного взаимодействия защитника и лиц, рассматривающих ходатайства и жалобы в уголовном судопроизводстве.

Такой системой электронного взаимодействия может стать Единый портал государственных и муниципальных услуг. Данный портал обладает высокой распространенностью среди граждан, используется на регулярной основе и не требует дополнительных навыков использования широким кругом лиц.

В соответствии с пунктом 7 статьи 2 Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» портал государственных и муниципальных услуг – 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.

На портале государственных и муниципальных услуг уже внедрено взаимодействие между гражданами и правоохранительными органами, что на первый взгляд должно упростить развитие портала в качестве системы, используемой для направления ходатайств и жалоб на стадии досудебного производства по уголовному делу, формирования системы электронного уголовного дела и электронного правосудия в уголовном судопроизводстве.

В данный момент на портале присутствует ряд функций в разделе «Правопорядок» на котором проработана возможность реализации некоторых услуг и функций.

В научных кругах считается, что внедрение информационной системы позволит провести оптимизацию деятельности органов предварительного расследования

(дознания), что может в наиболее сжатые сроки решить стоящие перед следователем (дознавателем) задачи [8. С. 8].

Но сможет ли раздел «Правопорядок» сайта «Госуслуги» быть доработан как целая отдельная информационная система? Является ли обработка жалоб и ходатайств в досудебном производстве государственной услугой и функцией в общем понимании данных понятий? Отвечает ли Единый портал государственных услуг всем требованиям информационной безопасности, позволяющим сохранить тайну следствия при направлении ходатайств и жалоб через сайт «Госуслуги»?

С целью ответа на вышеуказанные вопросы необходимо выявить правовую природу ходатайства и жалобы, понятия «государственная услуга», цели использования гражданами Единого портала государственных услуг как информационной системы, дающую возможность направлять электронные обращения.

Институт обжалования регулируется главой 16 УПК РФ, выделен как отдельный уголовно-процессуальный институт, обеспечивающий принцип состязательности уголовного судопроизводства и направленный на реализацию прав и законных интересов участников уголовного судопроизводства.

Институт ходатайств и жалоб представляет собой способ реализации права на обжалование процессуальных действий и решений, определяющих форму уголовного процесса. В принцип реализации права на обжалование включается и ходатайство как разновидность жалобы в уголовном судопроизводстве [7. С. 390].

Принимая во внимание, изложенное выше, можно сказать о том, что право на обжалование является отдельным процессуальным институтом. Реализация данного права в электронном виде через платформу обратной связи или раздел «Правопорядок» Единого портала государственных услуг представляется затруднительной. Кроме того, ходатайства и жалобы на стадии досудебного производства не могут рассматриваться в общем порядке, в соответствии с Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», в связи с тем, что согласно части 1 статьи 124 УПК РФ прокурор, руководитель следственного органа рассматривает жалобу в течение 3 суток со дня ее получения. В исключительных случаях, когда для проверки жалобы необходимо истребовать дополнительные материалы либо принять иные меры, допускается рассмотрение жалобы в срок до 10 суток, о чем извещается заявитель.

Наличие данной процессуальной нормы дополнительно подтверждает довод о нецелесообразности направления ходатайств и жалоб в электронном виде через Единый портал государственных услуг, порядок рассмотрения жалобы закреплен в уголовно-процессуальном законе, а не административным регламентом, что еще раз подтверждает обособленный института обжалования на стадии досудебного производства по уголовному делу.

Дополнительно стоит заметить, что в Российской Федерации высокий уровень киберпреступности, вопросы противодействия ей являются наиболее актуальными

в данный момент, в связи с чем использование Единого портала государственных услуг в качестве информационной системы, включающей в себя возможность направления ходатайств и жалоб на стадии досудебного производства затруднительно.

Не смотря на удобство использования цифровых сервисов, в современном мире многократно увеличилось число лиц, обладающих специальными знаниями в сфере компьютерной информации, которые в свою очередь объединяются в преступные группы и занимаются противоправной деятельностью, в том числе с использованием Единого портала государственных услуг [5. С. 150].

Исходя из вышеперечисленного, необходимо сделать вывод о том, что использование сайта «Госуслуги» в качестве информационной системы, позволяющей направлять ходатайства и жалобы на стадии досудебного производства нецелесообразно. Единый портал государственных услуг является неотъемлемой частью внедрение информационных технологий как в повседневную жизнь, так и в правовую сферу, но в настоящий момент не отвечает повышенным требованием информационной безопасности в уголовно-процессуальных отношениях.

С целью успешного внедрения электронного документооборота в уголовное судопроизводство необходимо создание отдельной информационной системы, которая будет представлять собой электронное уголовное дело, включать возможность направления в адрес органа, проводящего досудебное производство уголовного дела, доказательств в электронном виде. Важной частью системы электронного уголовного дела должна стать возможность обжалования действий (бездействия) должностных лиц в рамках статей 124 и 124 УПК РФ.

При внедрении в российское уголовно-процессуальное законодательство возможности ведения уголовного дела в электронном виде необходимо руководствоваться успешным опытом зарубежных стран с высокой долей информатизации уголовного процесса.

Опыт англо-саксонских стран наиболее показателен и успешен в данном направлении, некоторые процессы цифровизации уголовного судопроизводства являются уникальными и не имеют аналогов в процессуальном законодательстве других стран мира [13. С. 43].

Отдельно стоит выделить США, где уже успешно введена система электронного документооборота CM/ECF (Case Management and Electronic Case Files), посредством которой все доказательства, ходатайства и жалобы направляются непосредственно в адрес проводящего расследование уголовного дела органа, где они регистрируются и приобщаются к материалам уголовного дела. Все документы подаются в электронном виде в формате неизменяемого pdf файла, бумажные документы сканируются, для получения доступа к данной системе все участники уголовного судопроизводства регистрируются на специальном сайте, открывающим доступ к электронному уголовному делу [6. С. 71].

Стоит учесть, что российская система уголовного процесса нуждается в изменениях, внедрение электронного уголовного дела возможно на долгосрочной стадии развития досудебного производства. Данные теоретические представления уголовного процесса нереализуемы на практике и не соответствуют действующему уголовно-процессуальному законодательству, что исключает возможность электронного обжалования на стадии досудебного производства в настоящее время, следственно не может являться способом защиты подозреваемого (обвиняемого) по уголовному делу до полной проработки рассмотренных в исследовании вопросов.

Опыт зарубежных стран, несомненно, поможет в интеграции цифровизации досудебного производства в России, однако на пути его применения следует реформировать российское уголовно-процессуальное законодательство, закрепив в нем возможность направления документов в электронном виде через специальные информационные системы. Данные нововведения расширят возможности обжалования, что положительно скажется на развитии принципов уголовного судопроизводства.

Заключение. В ходе исследования использования электронного документооборота на стадии досудебного производства выявлен ряд научных и критических проблем, требующих проработки и решения.

Для полноценного расширения права на обжалование требуется корректировка уголовно-процессуального законодательства с целью внедрения цифровых приемов и способов направления ходатайств и жалоб именно на стадии досудебного производства по уголовному делу. Следует отметить, что в настоящее время не разработан механизм взаимодействия участников досудебного судопроизводства, также не в полной мере решен вопрос признания юридической силы ходатайств и жалоб, направляемых в электронном виде.

Выдвигаемые предложения по предоставлению электронной цифровой подписи нецелесообразны в связи с возможными ограничениями ее использования при осуществлении некоторых мер государственного принуждения в отношении подозреваемого (обвиняемого).

В процессе критического анализа выявлено отсутствие систематизации информационных ресурсов, дающих возможность направления электронных документов на стадии досудебного производства. Выдвигаемые научным сообществом предложения по реформации уже существующих цифровых платформ не подлежат применению на практике, так как обособленная роль уголовно-правовых отношений, включающих в себя государственное обвинение обуславливает собой необходимость создание отдельной системы с повышенными требованиями к информационной безопасности.

При внедрении информационных технологий в уголовное судопроизводства, необходимо использовать опыт зарубежных стран, в которых уже на достаточно

высоком уровне развит процесс обжалования незаконных действий (бездействия) должностных лиц на стадии досудебного производства по уголовному делу.

Учитывая сказанное выше, внедрение информационных технологий в уголовно-процессуальное право должно происходить постепенно с соблюдением принципов обоснованности и системности. В настоящее время важно придерживаться принятых процессуальных норм института обжалования, направленных на защиту прав и законных интересов, обеспечение принципов уголовного судопроизводства. Постепенное внедрение информационных технологий спровоцирует качественное развитие уголовного процесса, но только при параллельном развитии процессуальных норм, регулирующих цифовизацию уголовного процесса.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_34481 (дата обращения: 05.06.2025).

2. Федеральный закон от 25.12.2023 № 672-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_465608 (дата обращения: 06.06.2025).

3. Долгов А. М. Достижение назначения уголовного судопроизводства в условиях цифровизации уголовного процесса // Сибирские уголовно-процессуальные и криминалистические чтения. 2019. № 1(23) С. 56-59.

4. Гришин Д. А. Цифровизация досудебного уголовного судопроизводства // Вестник Томского государственного университета. 2020. № 455. С. 208–215.

5. Гонов А. М. Деятельность правоохранительных органов Российской Федерации по противодействию киберпреступности: правовые основы и проблемы правоприменения // Образование. Наука. Научные кадры. 2025. № 1. С. 148–154. https://doi.org/10.24412/2073-3305-2025-1-148-154. EDN: https://elibrary.ru/OQEXRT.

6. Ищенко П. П. Современные подходы к цифровизации досудебного производства по уголовным делам // Lex russica (Русский закон). 2019. № 12(157). С. 68-79. DOI 10.17803/1729-5920.2019.157.12.068-079. EDN TVXTXZ.

7. Максимов О. А. Место ходатайств и жалоб в современном уголовном процессе // Вестник Пермского университета. Юридические науки. 2021. Вып. 52. С. 372–393. DOI: 10.17072/1995-4190-2021-52-372-393.

8. Матросова Л. Д., Таршева М. Н., Кокин Д. М. К вопросу об использовании информационных технологий в отечественном уголовном процессе // Вестник Уральского юридического института МВД России. 2023. № 4. С. 5–10.

9. Меретуков Г. М., Грицаев С.И., Помазанов В.В. Актуальные вопросы цифровизации уголовного судопроизводства: взгляд в будущее // Правоприменение. 2022. Т. 6. № 3. С. 172–185.

10. Орешков И. А. Особенности использования современных информационных технологий в уголовном судопроизводстве РФ // Юристъ-Правоведъ : науч.-теоретич. и информац.-методич. журн. Ростов-на-Дону. 2024. № 1(108). С. 201-206.

11. Сергеев А.Б. «Цифровое» доказательственное право при производстве по уголовным делам о преступлениях в сфере компьютерной информации: вопросы целесообразности // Юридическая наука и правоохранительная практика. 2022. № 3 (61). С. 66-72.

12. Шестакова Л. А. Цифровизация уголовного судопроизводства отдельных стран континентальной Европы // Основы экономики, управления и права. 2023. № 1 (36). С. 89-93. doi:10.51608/23058641_2023_1_89.

13. Шестакова Л.А. Опыт использования информационных технологий в уголовном судопроизводстве отдельных стран англо-саксонского права // Основы экономики, управления и права. 2022. № 3 (34). С. 42-46. doi:10.51608/23058641_2022_3_42.

14. Щука И. О., Нестеренко О. С., Нестеренко Г. А.. Перспективы, достоинства и недостатки электронной подписи // Международный научно-исследовательский журнал. 2023. № 2(128). С. 1-3.

УДК 343

Ю.И. Селивановская,
кандидат юридических наук, доцент,
Казанский федеральный университет

Содержание понятия «киберпреступления» в контексте угроз экономической безопасности Российской Федерации

Аннотация. В статье рассматривается соотношение понятий «национальная безопасность», «экономическая безопасность» и «информационная безопасность». Одним из показателей состояния защищенности экономической безопасности Российской Федерации является уровень преступности в сфере экономики, а угрозой экономической безопасности нашего государства является высокий уровень экономической преступности. В данной статье выдвигается гипотеза о том, что и киберпреступления оказывают негативное влияние на экономическую безопасность Российской Федерации.

Ключевые слова: киберпреступление, преступление экономической направленности, национальная безопасность, экономическая безопасность, информационная безопасность

J.I. Selivanovskaya,
Candidate of Law, Associate professor,
Kazan Federal University

Content of the concept of "Cybercrime" in the context of threats to the economic secutity of the Russian Federation

Abstract. The article examines the relationship between the concepts of "national security," "economic security" and "information security." One of the indicators of the state of protection of the economic security of the Russian Federation is the level of crime in the economic sphere, and the threat to the economic security of our state is a high level of economic crime. This article hypothesizes that cybercrimes also have a negative impact on the economic security of the Russian Federation.

Keywords: cybercrime, economic crime, national security, economic security, information security

Введение. Обеспечение безопасности государства является приоритетной задачей Российской Федерации. Национальная безопасность - состояние защищенности национальных интересов от внешних и внутренних угроз. При этом в литературе активно обсуждается вопрос о разновидностях угроз национальной безопасности государства, и как следствии, о составляющих национальной безопасности. В частности, особый интерес представляет вопрос о соотношении понятий «экономическая безопасность» и «информационная безопасность».

В соответствии с пунктом 26 Указа Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [1] обеспечение и защита национальных интересов Российской Федерации осуществляются за счет концентрации усилий и ресурсов органов публичной власти, организаций и институтов гражданского общества на реализации следующих стратегических национальных приоритетов, в том числе информационной безопасности и экономической безопасности. То есть на сегодняшний день информационная безопасность и экономическая безопасность рассматриваются как равноправные составляющие национальной безопасности Российской Федерации. Д.М. Назаров и А.Д. Назаров отмечают, что «эти два понятия взаимосвязаны и влияют друг на друга, непосредственно и напрямую, так как угрозы информационной безопасности могут подорвать экономическую стабильность государства, нарушить его суверенитет, в то время как экономические кризисы влияют на способность общества обеспечивать информационную безопасность, потому что они ведут к сокращению инвестиций в технологии защиты информации» [2].

Однако такой подход существовал не всегда. Стратегия национальной безопасности Российской Федерации, действующая ранее, не выделяла информационную безопасность в качестве стратегического национального приоритета [3]. Это позволяло большинству авторов относить информационную безопасность к виду или элементу экономической безопасности [4].

Несмотря на придание самостоятельного значения информационной безопасности государства в разрезе национальных интересов, обеспечивать экономическую безопасность на должном уровне в условиях цифровой экономики без информационной составляющей невозможно. Например, в Стратегии экономической безопасности Российской Федерации на период до 2030 года [5] в качестве угрозы экономической безопасности относят не только подверженность финансовой системы Российской Федерации глобальным рискам (в том числе в результате влияния спекулятивного иностранного капитала), но также и уязвимость информационной инфраструктуры финансово-банковской системы.

Как известно, высокий уровень криминализации и коррупции в экономической сфере является угрозой экономической безопасности Российской Федерации. В связи с этим возникает вопрос, является ли киберпреступность угрозой экономической безопасности нашего государства.

Киберпреступность – это противоправная деятельность, совершаемая с использованием цифровых (информационно-телекоммуникационных) технологий. С.И. Буз отмечает, что «под «киберпреступлением» понимается любое преступление, совершенное с помощью информационных технологий, либо в информационном пространстве. При этом под информационными технологиями понимаются как технические средства (персональные компьютеры, ноутбуки, смартфоны), так и сама информация и ее носители. Под информационным пространством подразумеваются

информационно-телекоммуникационные сети (например, Интернет), компьютерные локальные сети и т. д. Специфика места совершения преступления обусловлена необходимостью использования специализированных инструментов (информационных технологий), что уже является основным признаком кибепреступления» [6].

В российском законодательстве не используется термин «киберпреступность». УК РФ предусматривает ответственность за совершение преступлений в сфере компьютерной информации. Однако, преступления, предусмотренные главой 28 УК РФ [7], это не единственные преступления в киберпространстве, ответственность за совершение которых предусмотрена уголовным законодательством России.

При формировании статистической отчетности используется более широкое понятие - преступления, совершенные с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации [8]. К данным преступлениям относятся, прежде всего, без дополнительных условий, следующие преступления: п. «г» ч. 3 ст. 158, ст. 159^3, 159^6, п. «в», ч. 3 и п. «в», ч. 5 ст. 222, п. «в» ч. 3 и п. «в» ч. 5 ст. 222^1, п. «в» ч. 3 и п. «в» ч. 5 ст. 222^2, п. «д» ч. 2 ст. 230, п. «г» ч. 2 ст. 242^2, ст. 272, 273, 274, 274^1, 274^2. Следует обратить внимание, что к данному перечню следует отнести и преступления, предусмотренные статьями 274^3-274^5 УК РФ (Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции, организация деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации, организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети «Интернет» для получения доступа к функциональным возможностям информационного ресурса) [9], которые были внесены в уголовное законодательство после принятия Указания Генпрокуратуры России № 462/11, МВД России от 25 июня 2024 г. № 2 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности». Как видим, к безусловным преступлениям, совершаемым с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации, относятся и экономические преступления – мошенничество с использованием электронных средств платежа, мошенничество в сфере компьютерной информации. Кроме того, к преступлениям, совершаемым с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации, относятся и иные экономические преступления при наличии определенного способа совершения преступления (с использованием сети «Интернет», с использованием электронных платежных систем и т.д.), такие как, например, фальсификация единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учета (ст. 170^1 УК РФ), легализация (отмывание) денежных средств или иного имущества, приобретенных

лицом в результате совершения им преступления (ст. 174[1] УК РФ), изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг (ст. 186 УК РФ).

Заключение. «Преступления в цифровом (кибер) пространстве и (или) с использованием цифровых технологий/систем/программ представляют естественную эволюцию преступности, обусловленную научнотехническим прогрессом и новыми разработками, и относятся к числу серьезных проблем современного мира» [10. С. 253]. Таким образом, как информационная составляющая играет важную роль в обеспечении экономической безопасности Российской Федерации, так и преступления, совершаемым с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации (киберпреступления), являясь одновременно и преступлениями экономической направленности, выступают угрозой экономической безопасности Российской Федерации.

Список литературы

1. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // Собрание законодательства РФ. 2021. № 27 (ч. II). Ст. 5351.

2. Назаров Д.М., Назаров А.Д. Анализ семантики понятий экономическая безопасность и информационная безопасность в цифровой экономике // Международный журнал прикладных наук и технологий INTEGRAL. 2023. № 4. URL: https://cyberleninka.ru/article/n/analiz-semantiki-ponyatiy-ekonomicheskaya-bezopasnost-i-informatsionnaya-bezopasnost-v-tsifrovoy-ekonomike?ysclid=mfbiagjfo0927459239 (дата обращения: 08.09.2025).

3. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31.12.2015 № 683 (утратил силу) // Собрание законодательства РФ. 2016. № 1 (ч. II). Ст. 212.

4. Ибрагимова З.М., Батчаева З.Б., Ткаченко А.Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона. 2022. № 11 (95). С. 26.-33.

5. О Стратегии экономической безопасности Российской Федерации на период до 2030 года: Указ Президента РФ от 13.05.2017 № 208 // Собрание законодательства РФ. 2017. № 20. Ст. 2902.

6. Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // Юристъ-Правоведъ. 2019. № 4 (91). С. 78-82.

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

8. О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: Указание Генпрокуратуры России № 462/11, МВД России № 2 от 25.06.2024 // СПС

«КонсультантПлюс» [Электронный ресурс]. URL: https://cloud.consultant.ru/cloud/cgi/online.cgi?req=doc&base=LAW&n=483902&dst=100001#KDDDEwUQLyJSG3up (дата обращения: 08.09.2025).

9. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2025 № 282-ФЗ // Собрание законодательства РФ. 2025. № 31. Ст. 4636.

10. Антонова Е.Ю. Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 251-269. https://doi.org/10.21202/jdtl.2023.10. EDN: HFPMTN

УДК 343.235

А. П. Серов,
адвокат Седьмой коллегии адвокатов Омской области

Использование сервисов VPN и прокси-серверов как обстоятельство, отягчающие наказание

Аннотация. В статье рассмотрено понятие и актуальные вопросы применения такого отягчающего наказание обстоятельства как совершение преступления с использованием программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен. Автор делает вывод, что вменение данного отягчающего обстоятельства возможно только в том случае, когда использование указанных средств облегчило или сделало возможным совершение лицом преступления.

Ключевые слова: уголовная ответственность, отягчающее обстоятельство, сервис VPN, прокси-сервер, средства преступления, орудия преступления, программно-аппаратные средства

A. P. Serov,
lawyer of the Seventh Bar Association of the Omsk region

Using VPN services and proxy servers as an aggravating circumstance

Annotation. The article discusses the concept and issues of the application of such an aggravating circumstance as the commission of a crime using software and hardware means of access to information resources, information and telecommunication networks, access to which is limited. The author concludes that the imputation of this aggravating circumstance is possible only if the use of these means facilitated or made it possible for a person to commit a crime.

Keywords: criminal liability, aggravating circumstance, VPN Service, proxy server, means of crime, instruments of crime, software and hardware

Введение. С 1 сентября 2025 г. вступили в силу изменения в Уголовный кодекс Российской Федерации, которые пополнили список отягчающих наказание обстоятельств следующим: «совершение преступления с использованием программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен». В настоящей статье рассмотрены понятие и актуальные вопросы применения такого отягчающего наказание обстоятельства.

Основная часть. К программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, относятся сервисы VPN и прокси-серверы.

Сервис VPN (с английского «Virtual Private Network» – «виртуальная частная сеть») представляет собой защищенный туннель, шифрующий интернет-трафик пользователя, направляя его через серверы виртуальной частной сети, которые расположены в различных точках мира. Тем самым VPN не только позволяет получить доступ к информации в сети Интернет, недоступной в регионе нахождения пользователя, но и маскирует IP-адрес, что делает следование за действиями пользователя практически невозможным для посторонних лиц [2. С. 191].

Прокси-сервер (от английского «proxy» – «представитель, уполномоченный») же, как следует из его названия, действует как посредник между сетью Интернет и устройством пользователя. Прокси-сервер передает запрос пользователя к интернет-ресурсу от своего имени, тем самым маскируя оригинальный IP-адрес, также как и VPN, обеспечивая анонимность и доступ к ограниченным в регионе сервисам [4. С. 283].

Использование вышеуказанных средств для совершения преступления возможно фактически при совершении любых деяний, которые возможно совершить при помощи информационно-телекоммуникационной сети Интернет.

Вместе с тем сразу же возникает вопрос допустимо ли вменение рассматриваемого отягчающего обстоятельства в случае, когда преступное деяние совершено с использованием сервиса VPN или прокси-сервера, но без получения доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен? Иными словами, данные программы не были отключены на устройстве пользователя, хотя необходимости в их использовании при совершении преступления не было.

Для ответа на данный вопрос необходимо обратиться к теории уголовного права.

Рассматриваемые программно-аппаратные средства относятся к средствам преступления. Под ними понимаются предметы, вещества и другие элементы, которые используются преступником для создания благоприятных условий осуществления преступления и облегчения его исполнения [3. С. 31].

Следовательно, функция средств преступления может выражаться либо в том, что они упрощают совершение преступления, либо делают его совершение возможным.

В отношении ресурсов и сетей, доступ к которым ограничен, сервисы VPN и прокси-серверы выполняют как раз функцию облегчения совершения преступления (поскольку возможность, например, размещения какой-либо информации на них возможно и без подобных программно-аппаратных средств, однако, для этого потребуется находится вне территории РФ).

Следовательно, когда преступление не совершено без доступа к заблокированным на территории РФ информационным ресурсам и информационно-телекоммуникационным сетям даже при наличии на устройстве лица, совершившего преступление, активированного сервиса VPN или прокси-сервера, данные программно-аппаратные средства не будут являться средствами преступления, поскольку никоим образом не упростили совершение преступления.

Здесь можно было бы возразить, что выше говорилось о наличии у сервисов VPN и прокси-серверов еще одной функции: обеспечение анонимности пользователя в сети. Может ли использование подобных программ для сокрытия личности преступника квалифицировано в качестве отягчающего обстоятельства?

На данный вопрос следует ответить отрицательно, поскольку в данном случае программно-аппаратные средства служат не совершению преступления, а его сокрытию, то есть средствами преступления не являются. Поскольку по действующему уголовному законодательству принятие мер к сокрытию преступления (применение перчаток, использование маски для сокрытия личности и пр.) не является отягчающим обстоятельством, то и в данном случае обеспечение анонимности в сети Интернет не должно влечь за собой ужесточение наказания.

Здесь следует отметить, что существуют многочисленные программно-аппаратные средства, направленные на выполнение подобной функции, именуемые, соответственно, анонимайзерами [1. С. 19]. При этом, данные программы могут и не выполнять функции доступа к заблокированным сетям и ресурсам.

Следовательно, если бы ответ на вопрос выше был бы положительным, то возникла бы парадоксальная ситуация: использование сервиса VPN или прокси-сервера для обеспечения анонимности при совершении преступления будет отягчающим обстоятельством, а использование анонимайзеров без функции доступа к заблокированным ресурсам и сетям для тех же целей на назначение наказания не влияет.

Заключение. До формирования стабильной судебной практики по вопросу квалификации рассматриваемого отягчающего обстоятельства адвокатам-защитникам по делам о преступлениях, совершенных с использованием сети Интернет, необходимо до первого допроса проконсультировать подзащитного относительно возможных вопросов о том, был ли активен сервис VPN или прокси-сервер на устройстве при совершении вменяемых деяний, поскольку не исключено, что основанием для внесения в обвинительный документ разбираемого отягчающего наказание обстоятельства могут стать исключительно показания самого обвиняемого.

Список литературы

1. Авласевич Д. В., Бачинский А. Г., Дмитриев Н. А., Кириллов А. А. Исследование принципов работы VPN, разработка политики безопасности VPN. Анонимайзеры и их применение // Форум молодых ученых. 2020. № 3 (43). С. 19-22.

2. Бадиков Д. А. Батуева А. Б. Проблемные вопросы раскрытия и расследования преступлений, совершенных с использованием VPN и proxy-серверов // Закон и право. 2025. № 1. С. 190-193.

3. Федышкина П. В. Соотношение орудий, средств и способа совершения преступления // КриминалистЪ. 2016. № 1 (18). С. 31-34.

4. Шоя А. А. Правовое регулирование сервисов VPN в контексте обеспечения соблюдения баланса интересов государства, общества и отдельно взятой личности в РФ // Международный журнал гуманитарных и естественных наук. 2024. № 10-5 (97). С. 283-286.

УДК 343.13

Н. А. Силантьева,
аспирант,
Сургутский государственный университет

Персональные данные в системе электронного мониторинга осужденных: правовые и информационные риски

Аннотация. В работе рассматриваются вопросы правового регулирования обработки и защиты персональных данных осужденных в условиях цифровой трансформации уголовно-исполнительной системы. Проведен анализ действующей нормативной базы, включающей федеральные законы, подзаконные и ведомственные акты, регулирующие применение электронного мониторинга. Установлено, что существующие механизмы носят фрагментарный характер и не обеспечивают комплексной защиты персональных данных осужденных, что формирует риски их неправомерного использования и утечек информации. Обосновывается необходимость законодательного закрепления специальных норм в Уголовно-исполнительном кодексе Российской Федерации и создание отраслевого стандарта технической защиты персональных данных.

Ключевые слова: уголовно-исполнительная система, цифровые технологии, электронный мониторинг, персональные данные осужденных, биометрические данные, право, информационная безопасность, правовое регулирование

N.A. Silanteva,
graduate student,
Surgut State University

Personal data in the electronic monitoring system of convicts: legal and informational risks

Abstract. Annotation. The paper examines the issues of legal regulation of the processing and protection of personal data of convicts in the context of the digital transformation of the penal system. The analysis of the current regulatory framework, including federal laws, by-laws and departmental acts regulating the use of electronic monitoring, is carried out. It is established that the existing mechanisms are fragmented and do not provide comprehensive protection of personal data of convicts, which creates risks of their misuse and information leakage. The necessity of legislative consolidation of special norms in the Penal Enforcement Code of the Russian Federation and the creation of an industry standard for the technical protection of personal data is substantiated.

Keywords: penal enforcement system, digital technologies, electronic monitoring, personal data of convicts, biometric data, law, information security, legal regulation

Введение. Министр юстиции Российской Федерации Константин Чуйченко на расширенном заседании коллегии ФСИН России в 2024 году определил приоритетные направления на 2025 год, среди которых продолжение работы в области цифровой трансформации [1].

Данный приоритет на уровне государственной политики непосредственно затрагивает уголовно-исполнительную систему, где внедрение цифровых средств контроля предполагает активную обработку персональных данных осужденных, отбывающих наказания без лишения свободы, поскольку именно в отношении данной категории лиц осуществляется наиболее масштабный сбор и хранение информации, включая биометрические и навигационные данные, что многократно увеличивает риски нарушения их прав и законных интересов.

Детальное понимание сущности электронного мониторинга требует обращения к действующим нормативно-правовым актам, закрепляющим основы его применения.

Основная часть. Значительное влияние на развитие электронного мониторинга оказал Федеральный закон от 27 декабря 2009 г. № 377-ФЗ [2]. Именно этот нормативный акт положил начало целенаправленному использованию электронных средств слежения в отношении лиц, приговоренных к наказаниям, не связанным с лишением свободы. Положения Уголовного кодекса Российской Федерации [13] формируют основу для законного использования данных средств слежения. В Уголовно-исполнительном кодексе Российской Федерации [14] прямо закреплена возможность применения аудиовизуальных, электронных и иных технических средств в процессе контроля за осужденными.

Значимым документом для практического применения цифровых технологий является приказ Министерства юстиции РФ от 11 октября 2010 г. № 258 [3], которым утверждена Инструкция по исполнению наказания в форме ограничения свободы. В данном акте содержатся ключевые процессуальные положения, регулирующие правила установки, эксплуатации и использования технических средств слежения, а также порядок их взаимодействия с осужденными.

Дополнительное регулирование обеспечивается актами Правительства Российской Федерации. Так, постановление Правительства Российской Федерации от 31 марта 2010 г. № 198 [10] закрепляется перечень устройств, разрешенных к использованию при электронном мониторинге (электронные браслеты, стационарные и мобильные комплексы контроля, ретрансляционные узлы, персональные навигационные трекеры), а в постановлении Правительства Российской Федерации от 18 февраля 2013 г. № 134 [4], уточняются правовые и процедурные аспекты использования аудиовизуальных и электронных средств в ходе применения меры пресечения в виде домашнего ареста.

Формирование системы правового регулирования в рассматриваемой области отражено и в Концепции развития УИС до 2030 года [5]. В данном документа акцентируется внимание на цифровой трансформации и внедрении инновационных

технологий, способствующих совершенствованию контроля и повышению уровня общественной безопасности.

Совокупность рассмотренных нормативных актов образует правовую основу для дальнейшего развития и совершенствования электронных средств контроля в уголовно-исполнительной системе. Вместе с тем, несмотря на наличие нормативно-правовой базы, действующее законодательство не обеспечивает комплексного и адаптированного к специфике уголовно-исполнительной системы регулирования вопросов, связанных с сохранностью и безопасной передачей информации, особенно по открытым каналам связи.

Так, Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [6] в статье 19 возлагает на оператора обязанность применять правовые, организационные и технические меры, направленные на обеспечение конфиденциальности персональных данных. Закон акцентирует внимание на необходимости защиты от несанкционированного доступа, утраты, изменения и других противоправных действий. Однако данные положения носят общий характер и не учитывают особенности информационного обмена в условиях режимных учреждений, а также риски, возникающие при использовании цифровых средств контроля, включая систему электронного мониторинга.

Аналогично, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [7] в статье 16 закрепляет общие подходы к защите информации от неправомерного вмешательства. Тем не менее, в нем отсутствуют положения, адресно регулирующие вопросы защиты персональных данных осужденных, особенно в условиях функционирования телекоммуникационных систем, применяемых в целях надзора и контроля.

Ведомственный приказ ФСИН России от 23 июня 2020 г. № 417 [8], несмотря на наличие определенных процедур обработки персональных данных в рамках уголовно-исполнительной системы, не содержит четких регламентов, касающихся технической защиты данных при их передаче с использованием современных электронных средств (например, браслетов, мобильных терминалов и других компонентов цифрового мониторинга). Отсутствие унифицированных требований к техническим и программным решениям оставляет возможность для потенциальных утечек информации и нарушений прав субъектов персональных данных.

В диссертации А.А. Сивцовой справедливо подчеркивается, что стремительное развитие цифровой среды формирует новые угрозы информационной безопасности в УИС, а защита персональных данных осужденных пока носит фрагментарный и недостаточно системный характер [11. С. 4].

Автор отмечает, что нормативная регламентация права осужденных на защиту персональных данных находится на начальном этапе своего становления, что связано с темпами цифровизации, опережающими процессы законодательного закрепления. Кроме того, отсутствует понятийный аппарат, позволяющий четко выделить

персональные данные осужденных как объект специальной защиты в уголовно-исполнительной системе, а также не выработаны эффективные механизмы предотвращения утечек и неправомерного доступа к информации.

Эти выводы представляются особенно значимыми применительно к практике использования электронных браслетов и иных систем мониторинга.

Таким образом, в настоящее время прослеживается очевидный правовой пробел: при наличии фрагментарных нормативных актов отсутствует единая, специализированная нормативно-техническая база, ориентированная на защиту персональных данных осужденных в условиях цифровой трансформации уголовно-исполнительной системы.

В этой связи, представляется целесообразным на законодательном уровне закрепить специальную статью в Уголовно-исполнительном кодексе Российской Федерации, регулирующую право осужденных на защиту персональных данных, а также устанавливающую ответственность за нарушения в данной сфере.

Такой подход был предложен в рамках разработки Общей части нового Уголовно-исполнительного кодекса Российской Федерации под научным руководством доктора юридических наук, профессора, заслуженного деятеля науки РФ В. И. Селиверстова [12. С. 42].

Для минимизации рисков нарушения конфиденциальности и утечек персональных данных целесообразно разработать и утвердить единый отраслевой стандарт технической защиты персональных данных, применимый ко всем цифровым системам контроля в Уголовно-исполнительной системы, а также закрепить в законе обязанность информирования осужденных о порядке обработки их персональных данных, включая права на доступ, исправление и обжалование неправомерных действий.

Дополнительные научные исследования также подтверждают высокую значимость специализированных механизмов защиты персональных данных в уголовно-исполнительной системе. Так, А.Д. Попова отмечает: «в связи с особенностями работы Федеральной службы исполнения наказаний информационная безопасность является критической составляющей: чтобы защитить конфиденциальность, целостность и доступность информации о персонале и операционных процессах, ФСИН России должна придерживаться строгих норм и правил в обеспечении информационной безопасности» [9. С. 51].

Заключение. В Российской Федерации создана нормативно-правовая база, регулирующая применение цифровых технологий контроля в уголовно-исполнительной системе. Однако действующее законодательство носит во многом общий характер и не учитывает специфики УИС, что приводит к правовым пробелам и рискам нарушения прав человека. Для обеспечения надежности цифровых систем надзора и повышения уровня правовой защищенности осужденных представляется необходимым закрепить специальные положения в Уголовно-исполнительном кодексе

Российской Федерации, разработать отраслевой стандарт защиты персональных данных и создать ведомственную модель угроз безопасности информации. Комплексное решение этих задач позволит реализовать стратегический курс государства на цифровую трансформацию и модернизацию уголовно-исполнительной системы.

Список литературы

1. Директор ФСИН России провел расширенное заседание по итогам работы ведомства // URL: https://clck.ru/3P4GMr (дата обращения: 28.08.2025).

2. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с введением в действие положений Уголовного кодекса Российской Федерации и Уголовно-исполнительного кодекса Российской Федерации о наказании в виде ограничения свободы: федеральный закон от 27.12.2009 № 377-ФЗ // Российская газета. 2009. 30 декабря.

3. Об утверждении Инструкции по организации исполнения наказания в виде ограничения свободы: приказ Минюста России от 11.10.2010 № 258 // Российская газета.

4. О порядке применения аудиовизуальных, электронных и иных технических средств контроля, которые могут использоваться в целях осуществления контроля за нахождением подозреваемого или обвиняемого в месте исполнения меры пресечения в виде домашнего ареста, а также за соблюдением возложенных судом запретов подозреваемым или обвиняемым, в отношении которого в виде меры пресечения избран запрет определенных действий, домашний арест или залог: постановление Правительства РФ от 18.02.2013 № 134 // Российская газета. 2013. 22 февраля.

5. О Концепции развития уголовно-исполнительной системы Российской Федерации на период до 2030 года: Распоряжение Правительства Российской Федерации от 29.04.2021 № 1138-р // Собрание законодательства РФ. 2021. № 20. Ст. 3397.

6. О персональных данных: федеральный закон от 27.07.2006 №152-ФЗ // Российская газета. 2006. 29 июля.

7. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 №149-ФЗ // Российская газета. 2006. 29 июля.

8. Об обработке персональных данных в уголовно-исполнительной системе Российской Федерации: приказ Федеральной службы исполнения наказаний от 23.06.2020 №417 // Официальном интернет-портале правовой информации (www.pravo.gov.ru) 25 августа 2020 г. № 0001202008250037.

9. Попова А.Д. Обеспечение информационной безопасности учреждений и органов уголовно-исполнительной системы Российской Федерации // Вестник Прикамского социального института. 2024. № 2 (98). С. 51-55.

10. Постановление Правительства Российской Федерации от 31.03.2010 №198 «Об утверждении перечня аудиовизуальных, электронных и иных технических средств надзора и контроля, используемых уголовно-исполнительными инспекциями для обеспечения надзора за осужденными к наказанию в виде ограничения свободы» // Российская газета. 2010. 7 апр.

11. Сивцова А.Ю. Право осужденных к лишению свободы на защиту персональных данных: нормативная регламентация и реализация : дис. ... канд. юрид. наук : 5.1.4 / Сивцова Анастасия Юрьевна. Рязань, 2024. 239 с.

12. Сивцова А. Ю. Проблемы правовой регламентации и реализации прав осужденных на защиту персональных данных // Ведомости УИС. 2018. № 6 (193). С. 39-42.

13. Уголовный кодекс Российской Федерации: Федеральный закон РФ от 13.06.1996 №63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

14. Уголовно-исполнительный кодекс РФ: Федеральный закон РФ от 08.01.1997 № 1-ФЗ // Собрание законодательства РФ. 1997. № 2. Ст. 198.

УДК 343.231:004.738

А. В. Скоробогатов,
доктор исторических наук, профессор,
Казанский инновационный университет
имени В. Г. Тимирясова

Метапреступность как социальное явление

Аннотация. Цель статьи состоит в комплексном исследовании природы метапреступности. На основе исследования отечественной и зарубежной литературы, посвященной изучению различных аспектов функционирования метавселенной и деяниям, нарушающим уголовно-правовые и социально-правовые запреты, обеспечивающие эффективность виртуальной коммуникации, автор рассмотрел понятие, элементы состава и значение метапреступности как социального явления. Сделан вывод, что двойственная природа метапреступности предполагает необходимость при квалификации противоправных деяний в виртуальной реальности учитывать нормы не только позитивного, но и социального права и обращать внимание на содержание, мотивацию и обстоятельства поведения субъекта и последствия деяния как в физическом мире, так и в пространстве метавселенной.

Ключевые слова: метапреступность, метавселенная, виртуальное пространство, уголовно-правовой запрет, цифровое право, состав преступления, таксономия метапреступлений

A.V. Skorobogatov
Doctor of History, Professor,
Kazan Innovative University named after V.G. Timiryasov,

Metacrime as a social phenomenon

Abstract. The aim of the article is to comprehensively study the nature of metacrime. Based on the study of domestic and foreign literature devoted to the study of various aspects of the functioning of the metaverse and acts that violate criminal and socio-legal prohibitions that ensure the effectiveness of virtual communication, the author examined the concept, elements of the composition and significance of metacrime as a social phenomenon. The article concludes that the dual nature of metacrime suggests the need to take into account the norms of not only positive but also social law when qualifying illegal acts in virtual reality and to pay attention to the content, motivation and circumstances of the subject's behavior and the consequences of the act both in the physical world and in the space of the metaverse.

Keywords: metacrime, metaverse, virtual space, criminal prohibition, digital law, corpus delicti, taxonomy of metacrimes

Введение. Современное общество переживает стремительно набирающую обороты революцию в области коммуникаций и информационных технологий, которую принято называть цифровой революцией. Технологический прогресс проник во все аспекты человеческой жизни, не оставив ни одной сферы, где бы технологии ни играли значительную роль в развитии социального бытия. Одним из наиболее результатов стали технологии искусственного интеллекта, кульминацией которых стало возникновение метавселенной, повлиявшей на жизнь человека на всех уровнях социальной, экономической и правовой реальности и проявилось в кризисе оптикоцентричного восприятия мира. Это обуславливает необходимость исследования этого явления не только с позиций информатики, но и в контексте современной гуманитаристики, в т.ч. различных вопросов правового регулирования.

Основная часть. Попытка синтезировать определения метавселенной, данные в научной литературе, позволила сформулировать следующую развернутую дефиницию: «Метавселенная представляет собой децентрализованную постоянную и иммерсивную трехмерную онлайн-среду, в которой пользователи, репрезентованные аватарами, могут креативно совместно участвовать в социальном и экономическом взаимодействии друг с другом в изолированных от физической реальности виртуальных пространствах» [16, p. 12373]. Фактически метавселенная представляет собой постреальность, в которой виртуальные и физические миры объединены в единую взаимосвязанную сеть, способствующую постоянному многопользовательскому взаимодействию.

Исходя из данного определения можно привести несколько признаков метавселенной, которые характеризуют ее вовлеченность в социальную и правовую коммуникацию: многопользовательская, многоцелевая, создаваемая пользователями, пространственная, иммерсивная, постоянная, многоплатформенная, интероперабельная, наличие владения или собственности на цифровые активы, наличие аватаров, синхронность, виртуально-физическая гибридность, открытость, децентрализованность, гиперпространственно-темпоральность, масштабируемость и неоднородность [13. P. 3]. Как иммерсивная онлайн-среда метавселенная по своей сути превосходит пространственные и временные ограничения, которые управляют межличностным взаимодействием в физическом мире. Во-первых, стираются национальные границы, и коммуникация все больше приобретает транснациональный характер [9. С. 131]. Во-вторых, благодаря иммерсивности постепенно стирается граница между реальным и виртуальным пространством [2]. В-третьих, цифровые аватары позволяют не только исследовать реальность прошлых эпох, но и приобрести чувства присутствия и сопричастности к деяниям прошлого. Тем самым можно говорить о синтезе в природе метавселенной виртуальности и иммерсивности, создающих не только возможности «инобытия» человека [1], но и воздействующих на ценностные ориентации и поведение в социальной реальности.

Наряду с позитивными последствиями, это порождает и негативные [5]. Технические решения, обуславливающие развитие метавселенной, не только имеют множество технологических и социальных уязвимостей, но и побуждают мотивированных преступников к активной их эксплуатации [12]. Речь при этом идет как о расширении пространства совершения уже имеющихся составов преступления за счет освоения виртуальных сред, так и о формировании новых составов, характерных исключительно для метавселенной.

Это предполагает необходимость не только введения новой категории «метапреступность», но и рассмотрение ее в широком социокультурном контексте. Главным при определении данного явления становится не юридические признаки (указание на противоправность деяния в нормативных правовых актах, прежде всего, в уголовном законе), а нарушение ими социального права (социальной конвенции, достигнутой субъектами, относительно коммуникативных ценностей и правил в метавселенной).

В самом общем плане метапреступления можно определить как противоправные деяния, которые могут совершаться в пространстве метавселенной [18. P. 9467]. Они представляют собой противоправное действие или бездействие, совершенное с использованием технических средств или устройств для автоматизированной обработки информации, независимо от того, способствовало ли это устройство совершению преступления, являлось ли оно местом преступления или служило средой для его совершения в закрытых или открытых информационных сетях [10. P. 177].

При определении объекта метапреступления целесообразно обратиться к аксиологическому подходу, в соответствии с которым к данному понятию относятся социальные ценности, охраняемые уголовным законом, на которые посягает лицо, совершающее преступление, и которым причиняется существенный вред в результате совершения данного деяния [8. С. 72]. Однако при этом необходимо учитывать, что имеющиеся пробелы в действующих нормах уголовного права относительно охраны общественных отношений в виртуальной среде предполагают расширительную интерпретацию понятия охраняемых социальных ценностей, включая в них не только то, что защищено непосредственно уголовно-правовыми запретами, но и те явления, которые получили защиту социального права, в т.ч. сконструированного непосредственно в метавселенной [7].

Хотя пространство метапреступлений, как явствует из приведенного определения, ограничиваются метавселенной, усложнение технических средств взаимодействия физического и социального мира позволило ряду ученых говорить о об отдельном типе «виртуально-физических» преступных деяний, при которых происходит использование цифровых моделируемых сущностей или датчиков виртуальной реальности для причинения не только психологического, но и физического вреда человеку в социальной реальности [13. P. 3].

Наиболее удачная таксономия метапреступлений была дана в отчете ИНТЕРПОЛА за 2024 г.: киберпреступность, финансовые преступления, имущественные преступления, сексуальные преступления и нападения, преступления против личности, терроризм, преступления против интеллектуальной собственности, преступления против детей, действия, направленные на то, чтобы вызвать страх или эмоциональный стресс, преступления против общественной безопасности [15]. В основу данной классификации был положен принцип modus operandi, позволяющий максимально полно охватить противоправные деяния в метавселенной. Несмотря не некоторые расхождения, в целом данного принципа классификации придерживается и научное сообщество [21]. Как видно из приведенного перечня к метапреступлениям могут быть отнесены как аналоги физических деяний, совершенные в метавселенной, так и специфичные деяния, не имеющие аналогов в физическом мире, а также деяния, совершение которых в виртуальной среде является продолжением действий индивида в социальной реальности.

Необходимо учитывать, что приведенный перечень не является закрытым и исчерпывающим. По мере того, как пространство метавселенной становится все более популярным, не только увеличивается количество метапреступлений, но и расширяется их таксономия, что влечет появление новых криминальных проблем.

Исходя из определения и таксономии метапреступлений, в качестве их объекта следует обозначить социально значимые ценности (материальные и нематериальные), на которые посягает лицо, совершающее преступление, и которым в результате деяния причиняется или может быть причинен существенный вред. Речь при этом может идти как о ценностях, существующих исключительно в виртуальной среде, так и о тех, которые существуют в физическом мире.

Более сложно определить субъекта метапреступлений. С одной стороны, классическая теория предполагает выделение в качестве такового исключительно дееспособного физического лица [3]. С другой стороны, необходимо учитывать все большее расширение значения искусственного интеллекта в качестве субъекта права [19]. При этом важно иметь в виду наличие возможной анонимности индивида в виртуальной среде. Речь может идти как о сокрытии своего «Я» цифровым аватаром, так и об использовании различных технических средств для анонимизации пользователя. Это не только затрудняет общеправовое определение субъекта преступления, но и существенно осложняет правоприменительную деятельность в данной сфере [11]. В самом общем плане субъекта метапреступления можно охарактеризовать как индивида, использующего возможности метавселенной для совершения деяний, противоречащих уголовному закону или нормам цифрового права. Поскольку в данном случае идет речь об использовании технических средств и навыков для доступа и совершения деяний в метавселенной, которыми как технически, так и организационно обладают не все лица, то нам представляется возможным говорить о специальном субъекте. В случае же анонимности лица речь должна идти о признании

субъектом индивида, который скрывается за анонимом или ответственен за создание технических средств анонимизации с использованием технологии искусственного интеллекта [20]. Однако говорить о необходимости введения уголовной ответственности для аватаров, как это предлагается в зарубежной литературе [21. P. 433], нам представляется нецелесообразным.

Объективной стороной метапреступления будет совершение противоправного деяния полностью или в значительной части в пространстве метавселенной, а также неправомерное использование физиологических и поведенческих биометрических данных неэтичными и злонамеренными способами. Хотя опасения по поводу неправомерного использования биометрических параметров не являются новыми этическими дилеммами в киберпространстве, функциональная совместимость и децентрализованные особенности метавселенной создают целевые возможности и огромные стимулы для мотивированных преступников инициировать неправомерное использование биометрических данных, особенно в отношении несовершеннолетних как одной из наиболее социально уязвимых и виртуально активных групп населения [14].

При характеристике субъективной стороны, наряду с признаками, выделяемыми современной криминологией применительно к классическим преступлениям, следует также рассматривать внешний вид и атрибуты цифровых аватаров, а также степень осознанности и целенаправленности выбора и использования индивидом образа в иммерсивной среде. При этом необходимо учитывать, что аватар выступает средством не только цифровой [6], но и социальной идентификации. Аватары позволяют пользователям создавать личности, которые могут отличаться от их личностей в социальной реальности, позволяя им менять свое поведение благодаря относительной анонимности и позволяя людям действовать способами, которые были бы невозможны или неприемлемы в офлайн-мире. По словам У. Шульце, аватар может быть либо репрезентативным (отражающим самоатрибуционные характеристики человека), либо перформативным (эксплицирующим выразительные, информативные и творческие составляющие личности человека) [17]. Происходит постепенное абстрагирование виртуальной коммуникации от фундаментальных нравственных ценностей, сопровождающееся не только формированием критического мышления [4], но и оказывающее существенное воздействие на отрицание индивидом преступного характера своего деяния. Кроме того, при квалификации метапреступлений следует учитывать степень осознанности нарушения индивидом уголовных запретов, поскольку зачастую использование дезинформации и искаженных данных происходит случайно, ситуативно, в силу недостаточной квалифицированности субъекта в определенном вопросе. Последний фактор особенно важен при квалификации деяний, совершенных несовершеннолетними лицами.

Заключение. Таким образом, метапреступность является специфичным правовым явлением, для определения которого необходимо не только синтезировать

уголовно-правовую и информационную науку, но и принципиально изменить общий подход к правовому регулированию. Двойственная природа метапреступности предполагает необходимость при квалификации противоправных деяний в виртуальной реальности учитывать нормы не только позитивного, но и социального права и обращать внимание на содержание, мотивацию и обстоятельства поведения субъекта и последствия деяния как в физическом мире, так и в пространстве метавселенной. Речь при этом может идти о сознании принципиально нового уголовного метаправа, создание которого должно осуществляться совместно государством, международными институтами, разработчиками технологий web 3.0 и сообществом пользователей.

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. DOI: 10.47475/2311-696X-2023-39-4-58-62.

2. Качалина Е.А., Тихомирова Е.Е. Категории пространства и времени в иммерсивном поле // Культурно-антропологические исследования. 2024. № 3. С. 8-22.

3. Назаренко Г.В. Субъект преступления: проблемы и решения. М.: Юрлитинформ, 2020. 176 с.

4. Напсо М.Б. Индивид в условиях виртуальной реальности // Человеческий капитал. 2024. № 4(184). С. 79-89. DOI: 10.25629/HC.2024.04.08.

5. Никульченкова Е.В. Трансформация киберпреступности: современные угрозы и их предупреждение // Вестник Омского университета. Серия: Право. 2023. Т. 20. № 3. С. 96-105. DOI: 10.24147/1990-5173.2023.20(3).96-105.

6. Петров П.К., Денисович В.В. Преступность в виртуальном пространстве: криминологическая характеристика // Проблемы права. 2025. № 1(97). С. 66-71. DOI: 10.14529/pro-prava250111.

7. Скоробогатов А.В. Цифровое право: в поисках баланса между реальностью и виртуальностью // Вектор развития управленческих подходов в цифровой экономике: Материалы III Всероссийской научно-практической конференции, Казань, 28 января 2021 года. Казань: Познание, 2021. С. 410-415.

8. Фесенко Е. Объект преступления с точки зрения ценностной теории // Уголовное право. 2003. №3. С. 71-73.

9. Шевко Н.Р., Лукина М.А. Киберпреступность: современное состояние и меры противодействия // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 130-133. DOI: 10.47475/2311-696X-2024-41-2-130-133.

10. Bensalem A.A., Bensadok A.. Gharbi A. Metaverse Technology and Criminal Law // Revue Des Sciences Humaines. 2025. Vol. 36. No. 2. P. 173-180.

11. Cheong B.C. Avatars in the metaverse: Potential legal issues and remedies. International Cybersecurity Law Review. 2022. Vol. 3(2). P. 467-494.

12. Dwivedi Y.K., Kshetri N., Hughes L. et al. Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse // Information Systems Frontiers. 2023. Vol. 25. P. 2071-2114. DOI: 10.1007/s10796-023-10400-x.

13. Gómez-Quintero Ju., Johnson Sh.D., Borrion H., Lundrigan S. A scoping study of crime facilitated by the metaverse // Futures. 2024. Vol. 157. P. 1-22. DOI: 10.1016/j.futures.2024.103338.

14. Horne C. Regulating rape within the virtual world // Lincoln Memorial University Law Review. 2023. 10(2). P. 159-176.

15. Metaverse: A law enforcement perspective. INTERPOL. [Электронный ресурс]. URL: https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf. Дата обращения: 25.07.2025.

16. Ritterbusch G.D., Teichmann M.R. Defining the metaverse: A systematic literature review // Ieee Access. 2023. Vol. 11. P. 12368-12377. DOI: 10.1109/ACCESS.2023.3241809.

17. Schultze U. Performing embodied identity in virtual worlds // European Journal of Information Systems. 2014. Vol. 23(1). P. 84-95. DOI: 10.1057/ejis.2012.52.

18. Seo S., Seok B., Lee C. Digital forensic investigation framework for the metaverse // The Journal of Supercomputing. 2023. Vol. 79. P. 9467-9485. DOI: 10.1007/s11227-023-05045-1.

19. Shen J. Can an Artificial Intelligence System Be Taken as a Legal Subject // Qingyang W., Zhang, LJ. (eds.) Services Computing – SCC 2022. SCC 2022. Lecture Notes in Computer Science. Vol. 13738. Cham: Springer, 2022. P. 12-25. DOI: 10.1007/978-3-031-23515-3_2.

20. Tiwari M., Lupton C., Bernot A., Halteh K. The cryptocurrency conundrum: The emerging role of digital currencies in geopolitical conflicts // Journal of Financial Crime. 2024. Vol. 31 (6). P. 1622-1634. DOI: 10.1108/JFC-12-2023-0306.

21. Zhou Y., Tiwari M., Bernot A. et al. Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality // Asian Journal of Criminology. 2024. Vol. 19. P. 419-439. DOI: 10.1007/s11417-024-09436-y.

УДК 343.1

Р. А. Танисов,
адъюнкт адъюнктуры,
Нижегородская академия МВД России

Алгоритмическое подозрение риски использования искусственного интеллекта в уголовно-процессуальной деятельности

Аннотация. В статье рассматриваются риски использования алгоритмических систем искусственного интеллекта в уголовно-процессуальной деятельности. В условиях стремительного развития технологий искусственный интеллект становится важной частью любой сферы жизнедеятельности общества, в том числе и рассматриваемой, в связи с чем его применение потенциально может влиять на соблюдение принципов справедливости, законности и защиты прав человека в уголовном процессе. Анализируются ключевые аспекты, такие как проблема предвзятости алгоритмов, непрозрачность решений искусственного интеллекта, угроза дискриминации и нарушение презумпции невиновности. Также изучаются этические, правовые и социальные последствия внедрения искусственного интеллекта в уголовно-процессуальную деятельность. В статье предлагаются рекомендации по минимизации рисков и обеспечению баланса между эффективностью технологий и защитой фундаментальных прав человека.

Ключевые слова: искусственный интеллект, уголовно-процессуальная деятельность, алгоритмическое подозрение, предвзятость алгоритмов, правовые последствия, прозрачность искусственного интеллекта, правовые последствия

R. A. Tanisov,
Associate Professor of Adjunct Studies,
Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia

Algorithmic suspicion of the risks of using artificial intelligence in criminal procedural activities

Abstract. The article discusses the risks of using algorithmic artificial intelligence systems in criminal procedural activities. With the rapid development of technology, artificial intelligence is becoming an important part of any sphere of society's life, including the one under consideration, and therefore its use can potentially affect compliance with the principles of justice, legality and protection of human rights in criminal proceedings. Key aspects such as the problem of algorithm bias, the opacity of artificial intelligence solutions, the threat of discrimination and violation of the presumption of innocence are analyzed. The ethical, legal and social consequences of the introduction of artificial intelligence in criminal procedure are also being studied. The article offers recommendations on minimizing risks and ensuring a

balance between the effectiveness of technology and the protection of fundamental human rights.

Keywords: artificial intelligence, criminal procedural activity, algorithmic suspicion, algorithm bias, legal consequences, transparency of artificial intelligence, legal consequences

Введение. Искусственный интеллект (далее – ИИ) представляет собой совокупность технологий, основанных на создании и использовании компьютерных систем, которые способны выполнять задачи, требующие человеческого интеллекта. В качестве основных можно выделить такие функции, как анализ данных, распознавание образов, обработка естественного языка, прогнозирование событий и принятие решений. В контексте уголовно-процессуальной деятельности ИИ становится мощным инструментом, способным существенно повысить эффективность и точность работы правоохранительных органов.

Основная часть. Как справедливо отмечают М.Н. Таршева и О.Д. Вастьянова, «основной принцип работы ИИ заключается в способности обрабатывать большие объемы информации, выявлять закономерности и делать выводы на основе анализа данных» [6. С. 270]. Достигается это благодаря использованию алгоритмов машинного обучения, которые позволяют системам обучаться на основе исторических данных и адаптироваться к новым условиям.

Исходя из выше приведенных аспектов, отражающих сущность ИИ, было сформулировано такое понятие как алгоритмическое подозрение. Это концепция, согласно которой подозрение в совершении преступления может быть сформировано на основе анализа данных, осуществляемого с использованием алгоритмов ИИ. В данном контексте под алгоритмом подразумевается программный код или модель машинного обучения, способная обрабатывать большие массивы информации, выявлять закономерности и делать выводы о возможной причастности лица к противоправной деятельности. Алгоритмическое подозрение предполагает, что решение о наличии признаков преступления или подозрении в отношении конкретного лица принимается не человеком, а системой, основанной на математических моделях и статистических данных.

На первый взгляд, внедрение алгоритмического подозрения может показаться шагом вперед в борьбе с преступностью. Однако его использование вызывает серьезные вопросы, касающиеся соблюдения прав человека и принципов уголовного процесса. По мере того как ИИ набирает силу, растет и потенциал его преступного использования [7. С. 67]. Одной из ключевых проблем является угроза презумпции невиновности. А.А. Ковалев, В.П. Тимофеев и И.Н. Шестаков в данном контексте подчеркивают, что «алгоритмы, даже самые продвинутые, не способны учитывать все обстоятельства дела и могут формировать подозрение на основе неполных или искаженных данных» [3. С. 115]. Данное обстоятельство создает риск того, что лицо

может быть необоснованно обвинено в совершении преступления без достаточных оснований.

Отдельно необходимо отметить, что алгоритмическое подозрение затрагивает право на защиту личной жизни. Для работы таких систем требуется сбор и анализ огромного количества данных, включая персональные сведения о гражданах. Данное обстоятельство способно привести к нарушению конфиденциальности и неправомерному вмешательству в частную жизнь. Также существует риск дискриминации, поскольку алгоритмы могут быть предвзятыми из-за особенностей обучающих данных.

В перспективе внедрение алгоритмического подозрения в уголовный процесс России требует тщательной оценки возможных последствий. На данный момент российское уголовно-процессуальное законодательство не предусматривает использование подобных технологий. Однако, внедрение несомненно потребует внесения изменений в Уголовно-процессуальный кодекс Российской Федерации, где должны быть четко прописаны основания и порядок применения алгоритмов, что также потребует разработки механизмов контроля за их использованием и защиты прав граждан.

Для более детального анализа возможностей внедрения алгоритмического подозрения в уголовный процесс России представим следующую таблицу (см. Таблица 1) [4. С. 113-114].

Таблица 1

Положительные и отрицательные стороны внедрения алгоритмического подозрения в уголовно-процессуальной деятельности

Аспект	Положительные стороны	Отрицательные стороны
Эффективность расследований	Ускорение анализа данных и выявления подозреваемых	Риск ошибок из-за ограниченности алгоритмов
Соблюдение прав человека	Возможность объективного анализа без человеческой предвзятости	Угроза презумпции невиновности и права на защиту личной жизни
Законодательная база	Возможность регулирования использования ИИ через законодательство	Необходимость внесения значительных изменений в УПК РФ
Технические аспекты	Развитие технологий ИИ в правоохранительной системе	Риск уязвимостей в программном обеспечении и утечек данных

Процесс интеграции ИИ в уголовно-процессуальную деятельность сопровождается множеством сложностей и особенностей. Данный процесс, как видно из таблицы, является многогранным. Учет правовых аспектов и социальных последствий весьма важны в данном вопросе. Только путем глубокого анализа и учета специфики интеграции ИИ возможно применять данный инструмент в обыденной практике весьма эффективно.

От того, насколько грамотно и успешно произойдет интеграция ИИ в правовую систему будет зависеть скорость расследований, точность анализа данных и выраженность доли человеческого фактора.

Предвзятость алгоритмов и риск возникновения ошибок возникают как одни из ключевых проблем использования искусственного интеллекта. И.В. Никифорова и А.И. Савельева утверждают, что ИИ обучается «на основе исторических данных, содержащих системные ошибки или проявления дискриминации» [5. С. 18]. Так, алгоритм может перенять тенденцию предвзятости в отношении отдельных социальных групп, если таковое встречалось в прошлом. Все это создает угрозу необоснованного подозрения или обвинения лиц.

К сожалению, сами алгоритмы могут стать угрозой защиты личной жизни. Кроме того, весьма сомнительны вопросы их надежности и безопасности, поскольку любые манипуляции порождают состояние уязвимости. Для работы ИИ требуется сбор и обработка большого объема данных, включая персональные сведения граждан. Данный аспект способен привести к нарушению конфиденциальности, а также обеспечить неправомерное вмешательство в частную жизнь.

Использование таких технологий без четко прописанных процедур и ограничений, в свою очередь, может привести к злоупотреблениям со стороны правоохранительных органов. К примеру, сбор данных о гражданах без их согласия или без достаточных оснований может быть расценен как нарушение конституционных прав.

Правовые аспекты регулирования использования ИИ в уголовно-процессуальной деятельности также остаются нерешенными. Российское уголовно-процессуальное законодательство на настоящий момент не содержит норм, разъясняющих применение данных технологий. «Отсутствие нормативной базы делает невозможным определение границ применения таких технологий, что в свою очередь увеличивает риск их неправомерного использования» [2. С. 171], отмечают О.И. Долгачева и Е.С. Кудряшова. Разработка норм, регулирующих все этапы применения ИИ, будут способствовать грамотному и эффективному их применению.

Пристального внимания требуют социальные последствия внедрения ИИ в уголовно-процессуальную деятельность. Повышение прозрачности и объективности работы правоохранительных органов, которое возможно при использовании искусственного интеллекта, положительно скажется на доверии со стороны общества.

Недоверие и страх перед новыми технологиями могут стать последствиями со стороны общественности. Все это приведет к росту социальной напряженности. В условиях ограниченности доступа к информации данная проблема будет лишь обостряться. Важно поддерживать уровень доверия к правовой системе в целом. Для этого эффективным методом будет проведение обучения как среди сотрудников, так и среди населения. Сама интеграция должна происходить постепенно.

Заключение. Использование ИИ сопряжено с множеством рисков. Особенно остро данный вопрос стоит в контексте уголовно-процессуальной деятельности. Среди таковых рисков можно отнести предвзятость, ошибки в работе алгоритмов, отсутствие прозрачности. Особенно актуальна проблема конфиденциальности личных данных.

Стоит также подчеркнуть, что существующее российское законодательство не готово к эффективному регулированию применения ИИ в этой сфере. Все это увеличивает риск проявления злоупотреблений ввиду правовой неопределенности. Грамотно разработанная нормативно-правовая база должна минимизировать риски алгоритмического подозрения.

Требуется усиление защиты персональных данных граждан и проведение просветительской работы среди населения. В условиях современного общества данный вопрос будет стоять весьма остро. Гарантия защита данных будет повышать авторитет правоохранительных органов и уровень доверия среди граждан.

Существенно повысить эффективность расследований способна интеграция технологий искусственного интеллекта в уголовной процесс России. Соблюдение ряда правовых и этических норм являются залогом успеха внедрения ИИ. Кроме того, важно подчеркнуть, что ведущую роль здесь играет комплексный подход. Помимо разработки нормативной базы и обеспечения прозрачности алгоритмов, необходимо информировать общество. Все это благоприятно скажется на успехе внедрения ИИ в уголовно-процессуальную деятельность.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (с изм. и доп. по состоянию на сентябрь 2025 г.) // Собрание законодательства РФ. 2001. № 52 (ч. I). Ст. 4921.

2. Долгачева О.И., Кудряшова Е.С. О возможности применения цифровых технологий и искусственного интеллекта в уголовном судопроизводстве // Научный вестник ОрЮИ МВД России им. В. В. Лукьянова. 2024. №2 (99). С. 168-175.

3. Ковалев А.А., Тимофеев В.П., Шестаков И.Н. Искусственный интеллект в уголовно-процессуальной деятельности: правовые основы и перспективы развития: монография / под ред. А.А. Ковалева. СПб.: Юридический центр Пресс, 2021. 278 с.

4. Кузнецов А.Г., Петрова Н.В. Риски использования искусственного интеллекта в правоприменительной практике // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. № 4 (60). С. 112-119.

5. Никифоров И.В., Савельев А.И. Проблемы применения технологий искусственного интеллекта в уголовном процессе Российской Федерации // Право и цифровая экономика. 2022. Т. 4, № 1. С. 15-26.

6. Таршева М.Н., Васьянова О.Д. Искусственный интеллект в борьбе с преступностью: уголовно-процессуальный и криминалистический аспекты // Научный вестник ОрЮИ МВД России им. В. В. Лукьянова. 2024. №3 (100). С. 266-275.

7. Бхатт Н. Преступления в эпоху искусственного интеллекта: гибридный подход к ответственности и безопасности в цифровую эру // Journal of Digital Technologies and Law. 2025. Т. 3, № 1. С. 65–88. https://doi.org/10.21202/jdtl.2025.3. EDN: rtolza.

УДК 343

А. Н. Тепленко,
соискатель кафедры уголовного права и процесса,
Казанский инновационный университет
имени В. Г. Тимирясова

Использование современных информационно-телекоммуникационных технологий для осуществления представительства иностранных граждан в уголовном судопроизводстве Российской Федерации

Аннотация. Данное исследование посвящено вопросу возможности использования современных информационно-телекоммуникационных технологий в уголовном судопроизводстве. Отмечается, что в процессе представительства иностранных граждан, выступающих в качестве участников уголовного судопроизводства, применение современных технологий будет способствовать развитию должной реализации представительских функций. Автором исследованы некоторые способы применения информационных технологий в процессе представительства иностранных граждан на примере использования специализированного программного обеспечения, видео-конференц-связи, электронного документооборота. В результате проведенного исследования делается обоснованный вывод о том, что комплексное исследование информационных технологий с позиции их использования в уголовном судопроизводстве позволит выявить полезные стороны применения данных технологий, оценить необходимость их внедрения в уголовный процесс и осуществить необходимую законодательную регламентацию такого применения в уголовном судопроизводстве.

Ключевые слова: представительство, представитель, представитель иностранного гражданина, представительство иностранных граждан, уголовно-процессуальное представительство, цифровое представительство, цифровизация, цифровизация уголовно-процессуального представительства, цифровизация уголовного судопроизводства, доступ к правосудию.

A. N. Teplenko
Candidate of the Department of Criminal Law and Procedure
Kazan Innovative University named after V. G. Timiryasov

Use of modern information and telecommunication technologies for representing foreign citizens in the criminal proceedings of the Russian Federation

Abstract. This study focuses on the possibility of using modern information and telecommunication technologies in criminal proceedings. It is noted that the use of modern technologies in the representation of foreign citizens as participants in criminal

proceedings will contribute to the proper implementation of representative functions. The author explores some methods of using information technologies in the representation of foreign citizens, such as the use of specialized software, video conferencing, and electronic document management. Based on the results of the study, it is concluded that a comprehensive study of information technologies from the perspective of their use in criminal proceedings will allow for the identification of the benefits of using these technologies, the assessment of the need for their implementation in the criminal process, and the necessary legislative regulation of their use in criminal proceedings.

Keywords: representation, representative, representative of a foreign citizen, representation of foreign citizens, criminal procedural representation, digital representation, digitalization, digitalization of criminal procedural representation, digitalization of criminal proceedings, access to justice.

Введение. В настоящее время процессы цифровой трансформации наблюдаются во всех направлениях общественной жизни. Не является исключением и проникновение высоких технологий в уголовное судопроизводство, что естественным образом вызывает необходимость в исследовании данного явления. Изучение процессов цифровизации отечественного уголовного права и процесса посвящены работы многих ученных. Так возможности применения технологий искусственного интеллекта подвергались исследованию И.Р. Бегишивым, З.И. Хисамовой [1, с. 192]. Правовым основам цифровой трансформации, правовому регулированию использования цифровых технологий, а также отдельным проблемам цифровизации и цифровой трансформации уголовного процесса посвящены исследования Д.В. Бахтеева, Е.А. Буглаевой, В.Б. Вехова С.В. Зуева [2, с. 176]. Вопросы применения информационных технологий в уголовном процессе рассмотрены в работах А.Ю. Чуриковой [3, с. 16-17]. Возможности внедрения и использования электронного документооборота освещались в трудах О.В. Мичуриной [4, с. 188]. Зарубежный опыт использования телекоммуникационных технологий в уголовном процессе анализировался научных изысканиях А.И. Трусова [5, с. 218].

Вместе с тем некоторые аспекты цифровой трансформации уголовного процесса остаются неизученными. Участие в уголовном судопроизводстве иностранного гражданина вносит в данный процесс большое количество особенностей и проблем, разрешение которых возможно посредством участия представителя [6, с. 428–429; 7, с. 83; 8, с. 22]. Вместе с тем, использование современных информационных технологий в осуществлении представительской деятельности иностранных граждан не подвергалось изучению, что обуславливает актуальность данного исследования и послужит развитию отечественного уголовно-процессуального права.

Основная часть. Рассмотрим некоторые направления возможного применения современных информационных технологий в обеспечении процесса участия представителя иностранного гражданина в уголовном судопроизводстве России.

Во-первых, вовлечение иностранного гражданина в качестве одного из участников уголовного судопроизводства России является одним из оснований для привлечения к участию его представителя. При должной законодательной регламентации использования современных технологий в уголовном процессе представитель иностранного гражданина будет иметь возможность оказать своевременную бесплатную юридическую помощь иностранному гражданину на любом этапе уголовного судопроизводства в том числе на этапе проведения процессуальной проверки сообщения о преступлении (ст. 144 УПК РФ).

Существующие проблемы процесса поиска и привлечения к участию представителя возможно обеспечить при помощи создания ведомственных или государственных интернет-платформ, юридических чатов, электронных юридических клиник, чат-ботов, колл-центров, юридических групп, сообществ и волонтерских организаций в целях оказания юридической и иной помощи и поддержки иностранным гражданам в вопросах участия в уголовном процессе.

Очевидно, что такого организации и системы должны быть законно созданы, финансово прозрачны и контролируемы надзирающими органами, а лица, выступающие в качестве представителей, установленным образом зарегистрированы в качестве представителей, имеющих необходимые и подтвержденные знания, навыки, практический опыт (например: знание иностранного языка, которое подтверждено соответствующим дипломом; знания или практический опыт в области юриспруденции с соответствующим подтверждением).

Кроме этого, следует рассмотреть возможность создания единых государственных реестров таких лиц, разделенных по категориям в зависимости от их возможностей, знаний, территориального расположения. При помощи специально разработанного программного обеспечения данные реестры можно внедрить посредством государственных или ведомственных интернет-сайтов, мобильных приложений, ссылок, которые могут быть предложены для ознакомления или установки на мобильные телефонные устройства иностранному гражданину в момент пересечения государственной границы Российской Федерации.

Применение указанных информационных технологий позволит существенно увеличить защиту прав и законных интересов иностранных граждан и обеспечить высокий уровень оказания своевременной и бесплатной юридической помощи и доступа к правосудию (п. 1 ч. 1 ст. 6 УПК РФ).

Во-вторых, при помощи внедрения и использования в уголовном судопроизводстве современных информационно-телекоммуникационных

технологий, таких как: видео-конференц-связь (ВКС) можно качественно решить существующие проблемы своевременности участия представителя иностранного гражданина в уголовном процессе.

Применение видео-конференц-связи должностным лицом, осуществляющим необходимые действия для обеспечения участия представителя, следует предусмотреть в любой момент и на любом этапе уголовного судопроизводства, в котором будет принимать участие иностранный гражданин. Посредством удаленного подключения представителя для проведения требуемых действий с участием иностранного гражданина можно решить ряд важных задач:

– оказание своевременной квалифицированной юридической помощи (например: консультации, разъяснение прав, обязанностей и последствий (ч. 1 ст. 11 УПК РФ);

– осуществление необходимого перевода устной речи или письменных документов иностранному гражданину и должностному лицу в процессе выполнения установленных законом действий (ч. 2 ст. 18 УПК РФ);

– присутствие и фиксация хода выполнения проводимых действий и принимаемых процессуальных решений в целях недопущения нарушений установленных процедур, порядка их проведения для предотвращения наступления возможных нарушений прав и законных интересов представляемого лица (ч. 3 ст. 7 УПК РФ);

– своевременное заявление необходимых ходатайств и подача жалоб на действия или бездействия должностных лиц или иных участников уголовного судопроизводства в интересах представляемого лица (ч. 1 ст. 19 УПК РФ);

– обеспечение безопасности участников уголовного судопроизводства путем проведения удаленных следственных действий или засекречивание лица (ч. 3 ст. 11 УПК РФ).

Разработка и использование государственных или ведомственных программных продуктов, внедрение которых в уголовный процесс позволит проводить необходимые сеансы связи между участниками уголовного судопроизводства, должны отвечать требованиям информационной безопасности, доступности, возможностям осуществления соответствующей верификации участников данного процесса.

Возможность быстрого привлечения к участию представителя без больших временных затрат позволяет своевременно принимать необходимые процессуальные решения, осуществлять требуемые организационные и процессуальные действия, что будет положительно влиять на полноту и своевременность проведения процессуальной проверки, предварительного расследования и судебного разбирательства (ч. 1 ст. 6.1 УПК РФ).

В-третьих, использование электронного документооборота в деятельности представителя иностранного гражданина существенно увеличит возможности

осуществления им своих представительских функций как участника уголовного процесса. Возможность оперативного и удаленного обмена необходимыми документами, в том числе относящимися к перечню доказательств, будет способствовать ускорению и удешевлению уголовного судопроизводства (ст. 74 УПК РФ).

Рассмотрим некоторые способы использования современных информационных технологий, связанные с электронным документооборотом при осуществлении представительских функций:

– направление электронным способом необходимых заявлений (ч. 1 ст. 144 УПК РФ), ходатайств (ч. 1 ст. 119 УПК РФ), жалоб (ч. 1 ст. 123 УПК РФ) в интересах представляемого лица;

– получения в электронным виде и в срок, установленный законом, повесток, копий принятых процессуальных решений и протоколов следственных и иных действий, уведомлений, писем, талонов-уведомлениий и иных документов, образующихся в процессе уголовного судопроизводства, в том числе обязательных для их вручения участникам (ч. 3 ст. 18 УПК РФ);

– получение и направление документов для осуществления перевода и документов, уже переведенных для иностранного гражданина на язык, которым он владеет (ч. 2 ст. 18 УПК РФ);

– получение и передача документов, необходимых для приобщения к материалам проверки сообщений о преступлении или к материалам уголовного дела (например: документы, удостоверяющие личность, знание языка, образование, регистрацию по месту жительства);

– применение возможностей электронной подписи в процессе осуществления уголовного судопроизводства (ч. 1 ст. 474.1 УПК РФ);

– возможность предоставления и сбора необходимых сведений и доказательств, имеющих значение в процессе уголовного судопроизводства (ч. 2 ст. 86 УПК РФ) [7, с 130-131].

Решение данных задач возможно посредством разработки и внедрения специализированного программного продукта, позволяющего безопасно, доступно и контролируемо осуществлять необходимое взаимодействие участников уголовного процесса (например: портал Госуслуги, официальные интернет-сайты, приложения МВД России, СК России, Прокуратура России).

Заключение.

Таким образом, использование современных информационных технологий при осуществлении представительских функций в отношении иностранных граждан, вовлеченных в уголовный процесс Российской Федерации, является действенной мерой по улучшению качества оказания юридической помощи, важным этапом модернизации и цифровизации уголовного процесса, который требует

комплексного научного исследования, практической апробации и законодательного закрепления.

Список литературы

1. Бегишев И.Р. Искусственный интеллект и уголовный закон // И.Р. Бегишев, З.И. Хисамова. – М.: Проспект. 2024. 192 с.

2. Правовые и организационно-технологические гарантии цифрового уголовного судопроизводства / Д.В. Бахтеев, Е.А. Буглаева, В.Б. Вехов [и др.]. – Москва: Издательский дом "Юрлитинформ", 2025. 312 с.

3. Чурикова А.Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование. автореф… дис. док. юрид. наук. – Саратов. 2024. С. 48.

4. Мичурина О.В. От бумажного к электронному документообороту: российский уголовный процесс в русле современных мировых тенденций // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: Материалы международной научно-практической конференции, Санкт-Петербург, 24 ноября 2023 года. – СПб: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2023. – С. 184-189.

5. Трусов А.И. Международный опыт применения телекоммуникационных технологий в уголовном процессе // Юристъ-Правовед: науч.-теоретич. и информац.-методич. журн. – Ростов-на-Дону. 2025. № 3 (114). С. 215–220.

6. Майоров А.В. Представительство иностранных граждан в уголовном судопроизводстве России // Социальное управление. 2025. Т. 7, С. 425–432.

7. Тепленко А.Н. Особенности содержания института представительства иностранных граждан в уголовном судопроизводстве Российской Федерации // Вестник Сибирского юридического института МВД России. 2025. № 2 (59). С.80–88.

8. Фойгель Е.И. Концептуальные основы криминалистического изучения этнических характеристик личности и практика их реализации в расследовании преступлений: автореф. дис. … д-ра юрид. наук: 12.00.12 / Е.И. Фойгель. Ростов-на-Дону, 2022. 54 с.

9. Мищенко Е.В., Никурадзе Г.О., Марина Е.А. К вопросу об использовании в уголовном процессе «электронных» доказательств. Санкт-Петербург. 2025. С. 128-132.

УДК 343.1

А. Н. Тепленко,
соискатель кафедры уголовного права и процесса,
Казанский инновационный университет
имени В.Г. Тимирясова

Представительство иностранных граждан в условиях цифровой трансформации уголовного процесса

Аннотация. В статье исследуются актуальные проблемы реализации института представительства иностранных граждан в уголовном судопроизводстве в условиях масштабной цифровизации правовой системы. Автор анализирует влияние цифровых технологий на процессуальное положение защитника и представителя иностранного гражданина, участвующего в уголовном процессе в качестве подозреваемого, обвиняемого или потерпевшего. Особое внимание уделяется проблемам реализации конституционного права на защиту в условиях внедрения электронного правосудия, дистанционного участия в процессуальных действиях посредством видео-конференц-связи и формирования электронного уголовного дела. В работе выявлены основные противоречия между требованиями процессуального законодательства о непосредственности судебного разбирательства и новыми формами цифрового взаимодействия участников процесса. Проведенное исследование показывает, что существующая нормативная база не обеспечивает должных гарантий процессуальных прав иностранных граждан в цифровой среде. Автор формулирует предложения по совершенствованию правового регулирования института представительства с учетом специфики правового статуса иностранных граждан и императивов цифровой трансформации уголовного судопроизводства.

Ключевые слова: уголовный процесс, представительство иностранных граждан, цифровизация правосудия, электронное уголовное дело, защитник, видео-конференц-связь, процессуальные права, цифровая трансформация, дистанционное участие

A. N. Teplenko
Candidate of the Department of Criminal Law and Procedure
Kazan Innovative University named after V.G. Timiryasov

Representation of foreign citizens in the context of the digital transformation of the criminal process

Annotation. The article examines the current problems of implementing the institution of representation of foreign citizens in criminal proceedings in the context of large-scale digitalization of the legal system. The author analyzes the impact of digital technologies on the procedural situation of a defender and representative of a foreign citizen participating in

criminal proceedings as a suspect, accused or victim. Special attention is paid to the problems of realizing the constitutional right to defense in the context of the introduction of electronic justice, remote participation in procedural actions through video conferencing and the formation of an electronic criminal case. The paper identifies the main contradictions between the requirements of procedural legislation on the immediacy of judicial proceedings and new forms of digital interaction between participants in the process. The conducted research shows that the existing regulatory framework does not provide adequate guarantees of the procedural rights of foreign citizens in the digital environment. The author formulates proposals for improving the legal regulation of the institution of representation, taking into account the specifics of the legal status of foreign citizens and the imperatives of the digital transformation of criminal proceedings.

Keywords: criminal procedure, representation of foreign citizens, digitalization of justice, electronic criminal case, defender, video conferencing, procedural rights, digital transformation, remote participation

Начать необходимо с констатации того факта, что современное уголовное судопроизводство переживает период радикальной трансформации под воздействием цифровых технологий. Как справедливо отмечается в научной литературе, цифровизация уголовного процесса представляет собой объективную реальность, определяющую вектор развития процессуального законодательства [1]. В этой связи представляет особый интерес проблема реализации института представительства иностранных граждан, находящихся в специфическом правовом положении участников уголовного судопроизводства.

Прежде всего обращает на себя внимание тот факт, что институт представительства в уголовном процессе традиционно основывался на принципе непосредственности и личного участия защитника в процессуальных действиях. Однако внедрение электронного правосудия существенно модифицирует классические представления о формах реализации защиты [2]. Особую актуальность данная проблема приобретает применительно к иностранным гражданам, которые зачастую не владеют языком судопроизводства, не знакомы с особенностями российской правовой системы и нуждаются в квалифицированной помощи представителя в условиях значительной географической удаленности от места производства по уголовному делу.

Наиболее существенным направлением цифровой трансформации выступает внедрение института дистанционного участия в процессуальных действиях посредством видео-конференц-связи. Как показывают исследования, использование видео-конференц-связи создает новые возможности для обеспечения права иностранного гражданина на защиту, позволяя осуществлять представительство без физического присутствия в зале судебного заседания [3]. Вместе с тем возникают серьезные вопросы о соблюдении адвокатской тайны, конфиденциальности общения защитника с подзащитным и возможности оказания эффективной юридической

помощи в условиях технически опосредованного взаимодействия. Наиболее сложным вопросом является обеспечение права на конфиденциальное общение с защитником, когда иностранный гражданин находится в изоляторе, а представитель участвует дистанционно.

Не менее существенно и то, что формирование электронного уголовного дела радикально изменяет механизмы ознакомления представителя с материалами расследования. Традиционная процедура ознакомления с материалами дела, предусмотренная ст. 217 УПК РФ, предполагала физическое присутствие защитника и возможность детального изучения всех документов [4]. В условиях цифровизации возникает возможность предоставления защитнику удаленного доступа к электронным материалам дела, что теоретически должно ускорить процесс и снизить процессуальные издержки. Однако применительно к представительству иностранных граждан данная трансформация порождает специфические проблемы, связанные с необходимостью обеспечения конфиденциальности информации, содержащейся в материалах дела, при ее передаче по электронным каналам связи за пределы территории Российской Федерации.

Следует особо отметить проблему идентификации и верификации полномочий представителя иностранного гражданина в цифровой среде. Действующее процессуальное законодательство требует предъявления ордера на исполнение поручения или доверенности для допуска защитника к участию в деле [5]. Вместе с тем в условиях электронного документооборота остается не выясненным вопрос о правовом признании электронных форм удостоверения полномочий представителя, особенно когда доверенность выдана в иностранном государстве и требует легализации или проставления апостиля. Таким образом, здесь налицо противоречие между требованием оперативности реализации права на защиту и формальными процедурами легализации документов, которые могут занимать значительное время.

Характерно также, что цифровая трансформация ставит под сомнение возможность полноценной реализации права иностранного гражданина на переводчика в условиях дистанционного участия. Принцип языка судопроизводства, закрепленный в статье 18 УПК РФ, гарантирует иностранному гражданину право пользоваться услугами переводчика. Однако при проведении процессуальных действий в режиме видео-конференц-связи возникают технические сложности обеспечения синхронного перевода, особенно когда участники процесса находятся в различных географических локациях [6]. Отсюда следует вывод о необходимости разработки специальных технических стандартов для обеспечения качественного перевода в условиях цифрового судопроизводства.

Отдельного внимания заслуживает проблема обеспечения процессуальных прав потерпевшего – иностранного гражданина в условиях цифровизации. В отличие от обвиняемого, который в силу применения меры пресечения физически находится на территории Российской Федерации, потерпевший может пребывать за рубежом. Это

создает объективные трудности для его участия в следственных действиях и судебном разбирательстве. Проведенные исследования показали, что существующие механизмы международной правовой помощи не адаптированы к реалиям цифрового судопроизводства и требуют значительных временных затрат, что может приводить к нарушению принципа разумного срока уголовного судопроизводства.

Весьма любопытно, что цифровизация создает новые возможности для транснационального представительства, когда адвокат, имеющий статус в иностранной юрисдикции, теоретически может оказывать юридическую помощь своему клиенту дистанционно. Однако действующее законодательство об адвокатуре устанавливает строгие требования к статусу защитника в уголовном процессе, ограничивая это право исключительно адвокатами, состоящими в адвокатских палатах субъектов Российской Федерации. Таким образом, цифровые технологии вступают в противоречие с национальным регулированием профессиональной деятельности, что требует выработки новых подходов к определению правомочий иностранных юристов в условиях цифровой трансформации.

В заключение необходимо подчеркнуть, что представительство иностранных граждан в условиях цифровой трансформации уголовного процесса нуждается в комплексном правовом регулировании. Представляется необходимым: во-первых, закрепить в процессуальном законодательстве гарантии конфиденциальности общения защитника с подзащитным при дистанционном участии; во-вторых, разработать механизмы признания электронных доверенностей, выданных в иностранных государствах; в-третьих, создать технические стандарты обеспечения синхронного перевода в цифровой среде; в-четвертых, определить правовой статус транснационального представительства с учетом цифровизации судопроизводства. Только системный подход позволит обеспечить эффективную защиту процессуальных прав иностранных граждан в условиях неизбежной цифровой трансформации уголовного правосудия.

Список литературы

1. Марковичева, Е. В. Влияние цифровых технологий на развитие уголовного судопроизводства / Е. В. Марковичева // Правосудие. – 2019. – Т. 1, № 1. – С. 98-107. – DOI 10.17238/issn2686-9241.2019.1.98-107. – EDN IALSGX.

2. Кононов, Д. А. Электронное правосудие в уголовном процессе в условиях цифровизации / Д. А. Кононов // Цифровое право. – 2025. – № 1. – С. 65-68. – DOI 10.24412/3034-4271-2025-1-65-68. – EDN HXSWRE.

3. Щербакова, А. В. Проблемы применения видео-конференц-связи в обеспечении адвокатом законных интересов подзащитного / А. В. Щербакова // Образование. Наука. Научные кадры. – 2025. – № 1. – С. 206-209. – DOI 10.24412/2073-3305-2025-1-206-209. – EDN KPSUAS.

4. Никурадзе, Н. О. Направления цифрового развития уголовного судопроизводства: позиции теории и практики часть I (электронное уголовное дело) / Н. О. Никурадзе, Е. В. Мищенко, Е. А. Марина // Право и государство: теория и практика. – 2025. – № 2. – С. 541-544. – DOI 10.47643/1815-1337_2025_2_541. – EDN QLJDWG.

5. Майоров, А. В. Представительство иностранного гражданина в уголовном судопроизводстве России / А. В. Майоров // Социальное управление. – 2025. – Т. 7, № 6. – С. 425-432. – EDN JIDSMB.

6. Кравченко, М. Е. Проблемы и перспективы цифровизации уголовного правосудия в Российской Федерации / М. Е. Кравченко, О. Д. Тупиха // Государственная служба и кадры. – 2025. – № 2. – С. 237-241. – DOI 10.24412/2312-0444-2025-2-237-241. – EDN MTULGZ.

УДК 343.3/343.9

Г. А. Тлепова,
соискатель степени PhD по праву,
Graduate University of Mongolia

Проблемы квалификации действий дропперов, ставших жертвами мошенничества

Аннотация. В работе рассмотрена актуальная проблема правовой оценки дропперов. На основе анализа судебной практики Казахстана выявлены различия в их субъективной оценке. Сравнительно-правовой обзор законодательства России, Германии и Сингапура выявил различия подходов правовой природы дропперов, от формального закрепления ответственности до учета неосторожного поведения при игнорировании подозрительных операций. Выделены критерии разграничения ответственности дропперов, закрепив в судебной практике и законодательстве.

Ключевые слова: дроппер, мошенничество, уголовная ответственность, правовая квалификация; жертва, судебная практика, Казахстан, сравнительно-правовой анализ, киберпреступность, уголовное право

G.A. Tlepova
PhD candidate in law,
Graduate University of Mongolia

Problems of qualification of actions of droppers who have become victims of fraud

Abstract. The paper examines the current issue of legal assessment of droppers. Analysis of Kazakhstan's judicial practice revealed differences in their subjective evaluation. A comparative review of Russian, German, and Singaporean law shows varying approaches to the legal nature of droppers – from formal liability to negligence when suspicious transactions are ignored. The author proposes criteria to distinguish liability and to entrench them in case law and legislation.

Keywords: dropper, fraud, criminal liability, legal qualification, victim, judicial practice, Kazakhstan, comparative legal analysis, cybercrime, criminal law

Введение

Цифровизация изменила общество открыв новые возможности во всех сферах жизни, но и породила новые формы преступности. Появился феномен использования так называемых «дропперов» – лиц, которые по тем или иным причинам предоставляют свои банковские реквизиты или счета для перевода и обналичивания средств, добытых преступным путем [13. P.12-14; 2].

Актуальность данной темы обусловлена тем, что отсутствует единообразный подход к квалификации дропперов. В одних случаях они рассматриваются как соучастники преступления, в других жертвами обмана. Такая двойственность приводит к правовой неопределенности и снижает доверие к правосудию.

Цель исследования выявить проблемы квалификации дропперов и выработать предложения по их устранению на основе анализа судебной практики Республик Казахстан и сравнительно-правового анализа законодательства России, Германии и Сингапура.

Научная новизна работы заключается в комплексном рассмотрении позиции дропперов не только как пособников, но и как возможных жертв мошенничества, что в свою очередь позволяет по-новому взглянуть на проблему квалификации и предложить системные решения.

Таким образом, введение в тему исследования показывает, что феномен дропперов требует не просто криминализации, сколько дифференциации ответственности в зависимости от формы вины.

Результаты исследования могут быть использованы в законотворчестве и при подготовке нормативных постановлений Верховного Суда РК.

Основная часть

Проблемы квалификации действий дропперов, ставших жертвами мошенничества

В июле 2025 года в Республике Казахстан был принят закон, которым в Уголовный кодекс впервые введена самостоятельная уголовная ответственность за так называемых дропперов [9]. Эти изменения вступают в силу 16 сентября 2025 года и знаменуют собой новый этап эволюции национальной уголовной политики. Если ранее действия подобных лиц квалифицировались лишь в рамках общих положений о соучастии (статья 28 УК РК) и мошенничестве (статья 190 УК РК), то теперь законодатель прямо закрепил ответственность за использование и предоставление банковских счетов, карт или электронных кошельков для обналичивания и перевода денежных средств, добытых преступным путем.

Феномен «дропперов» является сравнительно новым для отечественной уголовно-правовой практики, но уже приобрел широкое распространение в условиях цифровизации финансовых отношений. Под дропперами принято понимать физических лиц, которые предоставляют свои банковские карты, реквизиты счетов или электронные кошельки для перевода и обналичивания денежных средств, добытых преступным путем. При этом субъективное восприятие таких лиц может существенно различаться от сознательного пособничества организованным преступным группам до введения их в заблуждение мошенниками.

Термин «дроппер» заимствован из англоязычной практики противодействия киберпреступности, где используется понятие money mule – «денежный мул» [14. С.702]. Первоначально оно применялось в криминалистике для обозначения

посредников, участвующих в отмывании похищенных средств. В казахстанской юридической литературе термин пока не получил официального закрепления, однако активно используется исследователями и практиками при описании новых форм мошенничества, совершаемых с использованием информационных технологий.

При этом принципиально важно отметить, что субъективная сторона поведения дроппера неоднородна. Часть таких лиц действует умышленно, осознавая преступный характер содеянного и получая вознаграждение, другая часть вводится в заблуждение, и сама становится жертвой мошенничества.

Феномен дропперов в последние годы приобрел массовый характер не только в Казахстане, но и в других странах. Правоохранительные органы фиксируют устойчивый рост числа мошенничеств, связанных с переводами денежных средств через подставные счета [8. С.120-125]. Типичный способ вовлечения граждан строится на методах социальной инженерии, в виде объявления «о легком заработке», поддельные звонки «сотрудников банка» или предложение оформить счет для «временного хранения средств» и другие способы. По этой причине тысячи граждан оказались в ситуации, когда они одновременно могут рассматриваться и как жертвы обмана, и как посредники в схемах преступников [1. С. 45; 7. С.118].

Для феномена дропперов можно выделить ряд признаков, таких как посреднический характер, использование цифровых технологий и вариативность субъективной стороны.

Даже после введения уголовной ответственности за дропперов остается открытым вопрос, как отграничить умышленное пособничество от ситуаций, когда лицо было жертвой обмана. Именно эта проблема становится предметом научной дискуссии и судебных коллизий, требующих доктринального осмысления и разъяснения со стороны Верховного Суда Республики Казахстан.

В ходе исследования были проанализированы судебные дела, размещенные в Информационной системе «Төрелік», так по уголовным делам суды Казахстана дропперы всегда признавались как пособники или соисполнители преступлений.

Показательно дело Нүсіпбекова, в котором подсудимый заявлял о виктимности, однако из судебного акта следует, что его поведение активно, он самостоятельно создал криптокошельки, управлял паролями и контролировал транзакций, послужило для суда достаточным основанием признания его виновным в совершении мошенничества и квалификации по пункту 2) части 4 статьи 190 УК РК [3].

Подобные выводы были сделаны судом в деле Журмана и других, деяния которых квалифицированы как пособничество в мошенничестве [10].

В деле Утемисова и Лима была использования классическая схема совершения интернет – мошенничества, где переправление поступивших денежных средств на криптокошельки за вознаграждение указывал на их прямой умысел [5].

Подытоживая сказанное, можно сделать вывод, что в рамках судопроизводства по уголовным делам сложилась устойчивая тенденция, когда действия в виде передачи

реквизитов или участие в транзакциях расценивается умышленным содействием, доводы же о виктимности отвергаются.

Иная картина сложилась по гражданским делам, иски о взыскании неосновательного обогащения удовлетворялись в случае отсутствия оснований у ответчика для получения денежных переводов. Однако если потерпевший производил операции по обмену криптовалют, то исковые требования признавались необоснованными.

Показателен пример по иску Однодворского к банку о признании сделки банковского займа недействительной. В 2022 году он заключил договор займа на 1,5 млн тенге, полученные средства по указанию мошенников перевел на счета третьих лиц. По жалобе Однодворского правоохранительными органами начато досудебное расследование по факту мошенничества, в рамках которого он признан потерпевшим.

Иски Однодворского о взыскании неосновательного обогащения с третьих лиц удовлетворены частично, поскольку у двух ответчиков не было оснований для получения средств, а деньги ими были переведены на другие счета. По иску о взыскании с третьего лица отказано, поскольку переводы носили характер «биржевых сделок» с криптовалютой, что было подтверждено выписками с банка [6].

Верховный суд по данному делу признал необоснованными требования истца о признании сделки банковского займа, так как Однодворский лично совершил действия через свой мобильный телефон, затем перевел деньги на банковские счета третьих лиц [2].

Сравнительный анализ судебной практики по уголовным и гражданским делам показывает, что в уголовном судопроизводстве дроппер, это пособник или соисполнитель, а в гражданских делах они оцениваются как жертвы, лишенные имущественной выгоды. Проведенное обобщение позволяет констатировать о наличии двойственности в оценки действий дропперов.

Такая двойственность оценки действий подрывает единообразие правоприменения и принцип виновной ответственности.

Автор считает, что выход из сложившейся ситуации возможен путем принятия нормативного постановления Верховного Суда РК, где должны быть зафиксированы признаки, по которым можно отличать умышленное пособничество, выраженное в системности, выгоде и осведомленности, от поведения лица, введенного в заблуждение.

Сравнительно-правовой анализ проведен по законодательству России, Германии и Сингапур. Выбор государств обусловлен различными факторами, так Россия как ближайшее государство с общей правовой традицией и схожими проблемами квалификации преступлений, совершаемых с применением информационных технологий.

Германия выбрана для анализа, поскольку является представителем развитой континентальной системой, при этом их модель заимствована Казахстаном при принятии уголовно-процессуального и уголовного законодательства.

Выбор Сингапура связан с тем, что страна придерживается юрисдикции англосаксонского права, также является одним из признанных мировых лидеров в сфере цифрового регулирования и противодействия киберпреступлениям.

Как и в Казахстане до середины 2025 года российское законодательство не содержало специального состава о дропперах. Их действия квалифицировались как пособничество в мошенничестве (статья 159 УК РФ), легализация преступных доходов (статья 174 УК РФ) либо незаконный оборот средств платежей (статья 187 УК РФ). Такая квалификация приводила к неустойчивой практике, в одних случаях признавали дропперов жертвами, в других – соучастниками преступлений [4].

Россия, немного опередив Казахстан приняла Федеральный закон, вступивший в силу 5 июля 2025 года, которым была установлена уголовная ответственность за передачу платежных инструментов или их реквизитов для совершения преступлений. Таким образом, Россия одной из первых закрепила самостоятельный состав за дропперство, однако вопрос о разграничении умысла и заблуждения остался еще открытым.

В немецком праве отсутствует отдельная статья о дропперах, однако норму УК (StGB) охватывают этот феномен по разным составам правонарушения, такие как § 263 StGB (мошенничество), § 263a StGB (компьютерное мошенничество) и § 261 StGB (отмывание денег).

Особенностью § 261 StGB является то, что он предусматривает ответственность не только при умышленных действиях, но и при грубой неосторожности (leichtfertige Geldwäsche). Это позволяет привлекать к ответственности Finanzagenten (финансовых агентов, или money mules), даже если они не имели прямого умысла, но проявили очевидную беспечность – например, предоставили свой счет за комиссию, не поинтересовавшись происхождением средств [15].

По мнению автора Германская модель является оптимальной, поскольку демонстрирует гибкость, умышленные действия квалифицируется как пособничество, а неосторожные как форма отмывания

Сингапурская модель более усовершенствована. В феврале 2024 года были внесены изменения в Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act CDSA, так были введены два новых состава, направленных на пресечение массового вовлечения граждан в схему money mules [12].

Первое, rash money laundering – когда лицо имело основания подозревать незаконность транзакций, но все равно ее совершило.

Второе, negligent money laundering – когда лицо проигнорировало очевидные «красные флаги» (признаки подозрительных операций: быстрый заработок за

предоставление карты, переводы от неизвестных лиц и т.п.) без должной проверки [11; 12].

Новелла в Казахстане устранила прежнюю неопределенность, когда дропперы квалифицировались как пособники в мошенничестве или легализации и закрепила самостоятельный состав.

Автор полагает, что для Казахстана необходимо учитывать зарубежный опыт, поскольку уголовный закон должен не только наказывать умышленных пособников, но и содержать механизмы защиты лиц, фактически ставших жертвами мошеннических схем. Сопоставительный анализ правовых моделей Германии, Сингапура и России позволяет сформулировать вывод о целесообразности адаптации отдельных элементов в отечественном законодательстве, с возможностью введения ответственности за передачу счетов третьим лицам при отсутствии прямого умысла.

В казахстанской судебной системе выявлено двойственное отношение к дропперам, если в уголовных делах их относят к пособникам мошенников, то в гражданских процессах те же самые люди нередко признаются жертвами. Это в свою очередь подрывает принцип виновной ответственности и демонстрирует отсутствие единообразия в правоприменении.

Принятый в июле 2025 года закон, закрепивший самостоятельный состав преступления за деятельность дропперов, стал важным шагом. Однако он решает только часть проблемы, поскольку охватывает лишь умышленные действия, но не дает ясных критериев, как отличить сознательное пособничество от ситуации, когда человек сам введен в заблуждение и не извлекает выгоды. Из-за этого сохраняется риск уголовного преследования тех, кто объективно является потерпевшим.

На практике остаются без ответа следующие ключевые вопросы, считать ли извлечение выгоды главным доказательством умысла, относится к единичным эпизодам передачи реквизитов под давлением обмана, должна ли простая небрежность, например игнорирование «красных флагов», влечь уголовную ответственность или быть отнесена к сфере административного права.

Сравнительный анализ законодательства показал, что Германия и Сингапур используют более гибкие модели. В Германии предусмотрена ответственность и за грубую неосторожность, что позволяет охватывать широкий спектр поведения. В Сингапуре введены категории rash и negligent money laundering, обеспечивающие возможность привлечения лиц, игнорирующих очевидные «красные флаги».

Для Казахстана этот опыт может быть полезен, однако его механическое заимствование нежелательно, поскольку чрезмерная криминализация может привести к неоправданному преследованию добросовестных граждан, так как массовое вовлечение граждан связана с активной цифровизации во всех сферах жизни.

Автор полагает, что для устранения выявленной правовой неопределенности необходимо принять нормативное постановление Верховного Суда Республики Казахстан, закрепляющего критерии разграничения статуса дропперов и ввести

административную ответственность за неосторожное поведение. Предложения носят дискуссионный характер и отражают авторскую позицию, что подчеркивает научную новизну исследования.

Заключение

Проведенное исследование выявило, что ключевая трудность в квалификации дропперов заключается не столько в отсутствии уголовно-правовой нормы, сколько в неопределенности их правового статуса. В одних случаях они выступают как соучастники, в других – как потерпевшие.

Анализ зарубежных подходов свидетельствует, что каждая страна идет своим путем, но имеет общую тенденцию, где ответственность дифференцируется с учетом субъективной стороны деяния. Германия и Сингапур сделали шаг в сторону привлечения к ответственности и за грубую неосторожность, в то время как Россия и Казахстан ограничились умышленными действиями.

Автор полагает, что для Казахстана оптимальным является комбинированный путь, а именно сохранить строгую ответственность для умышленных пособников и одновременно закрепить защитные механизмы для тех, кто оказался жертвой.

Представляется, что решение данной проблемы возможно не только через судебное разъяснение и выработку единых критериев разграничения виновного соучастия и добросовестного заблуждения, но и посредством закрепления административной ответственности за неосторожные действия дропперов.

Научная новизна исследования заключается в следующем.

Во-первых, проведен системный анализ противоречий между уголовно-правовой и гражданско-правовой оценкой статуса дропперов в судебной практике Казахстана.

Во-вторых, предложены четкие критерии разграничения оценок – включая наличие выгоды, систематичность и осведомленность лица.

В-третьих, обоснована необходимость издания нормативного постановления Верховного Суда РК для унификации квалификации дропперов, а также введения административной ответственности за использование и предоставление банковских счетов, карт или электронных кошельков для обналичивания и перевода денежных средств, если эти действия не содержат признаки уголовно наказуемого деяния.

Список литературы

1. Нуртаева Ж. С. Информационная безопасность и уголовная ответственность. Алматы: Жеті Жарғы, 2022. 215 с.

2. Постановление судебной коллегии по гражданским делам Верховного Суда Республики Казахстан по делу № 6001-25-00-3г/1162 по иску Однодворского от 7 апреля 2025 г. [Электронный ресурс]. Режим доступа: закрытая информационная система «Төрелік»

https://torelik.sud.kz/#/court/caseinstance/info/22234827012?tab=cover-letter-file (дата обращения: 25.08.2025).

3. Постановление судебной коллегии по уголовным делам Алматинского городского суда по делу № 7599-24-00-1а/73 в отношении Нүсіпбекова от 14 февраля 2024 г. [Электронный ресурс]. Режим доступа: закрытая информационная система «Төрелік» https://torelik.sud.kz/#/court/caseinstance/info/20584281703?tab=cover-letter-file (дата обращения: 25.08.2025).

4. Приговор межрайонного суда по уголовным делам г. Астаны по делу № 7141-23-00-1/457 в отношении Журмана и др. от 19 октября 2023 г. [Электронный ресурс]. Режим доступа: закрытая информационная система «Төрелік» https://torelik.sud.kz/#/court/caseinstance/info/20005730410?tab=cover-letter-file (дата обращения: 25.08.2025).

5. Приговор районного суда № 2 Медеуского района г. Алматы по делу № 7525-25-00-1/113 в отношении Утемисова и Лима от 19 марта 2025 г. [Электронный ресурс]. – Режим доступа: закрытая информационная система «Төрелік» https://torelik.sud.kz/#/court/caseinstance/info/22275088832?tab=cover-letter-file (дата обращения: 25.08.2025).

6. Решение Костанайского городского суда по делу № 3910-24-00-2/3039 по иску Однодворского о признании сделки недействительной от 13 ноября 2024 г. [Электронный ресурс]. – Режим доступа: закрытая информационная система «Төрелік» https://torelik.sud.kz/#/court/caseinstance/info/21614583297?tab=cover-letter-file (дата обращения: 25.08.2025).

7. Сапаргалиев Г. С. Проблемы квалификации ИТ-преступлений // Право и государство. 2023. № 4. С. 112–125.

8. Трофимов Д. А. Киберпреступность и уголовное право. – М.: Юрлитинформ, 2021. 340 с.

9. Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V ЗРК (с изм. и доп. по состоянию на июль 2025 г.) [Электронный ресурс]. – Режим доступа: https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения: 25.08.2025).

10. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с изм. и доп. по состоянию на июль 2025 г.) [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 28.08.2025)

11. Computer Misuse Act 1993 (Singapore) [Электронный ресурс]. Режим доступа:https://sso.agc.gov.sg//Act/CMA1993?ViewType=Advance&Phrase=Computer+Misuse+Act&WiAl=1 (дата обращения: 25.08.2025).

12. Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Singapore, amendments of 2024) [Электронный ресурс]. Режим доступа:https://sso.agc.gov.sg//SL/CDTOSCCBA1992-S6-

2015?DocDate=20230707&ViewType=Advance&Phrase=Corruption%2c+Drug+Trafficking+and+Other+Serious+Crimes&WiAl=1(дата обращения: 25.08.2025).

13. International Telecommunication Union. Global Cybersecurity Index 2023 [Электронный ресурс]. Geneva: ITU, 2023. 76 p. Режим доступа: https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx (дата обращения: 25.08.2025).

14. Levi M. Money mules as facilitators of fraud and money laundering // Journal of Financial Crime. 2021. Vol. 28, № 3. P. 699–715.

15. Strafgesetzbuch (StGB). –German Criminal Code. München: C. H. Beck, 2024.– 524 p.

УДК 343.2/.7

Е. В. Фокина,
кандидат экономических наук,
Ростовский государственный экономический университет (РИНХ),
филиал в г. Ейске, Краснодарский край

Уголовно-правовые пределы регулирования побочных эффектов научно-технического развития

Аннотация. Научно-технический прогресс демонстрирует экспоненциальную динамику развития, опережая адаптационные возможности правовых институтов. В статье анализируется феномен «побочных эффектов» технического прогресса как источника киберпреступности, выявляются структурные пределы уголовного законодательства в управлении технологическими рисками, обосновывается переход от репрессивной модели к риск-ориентированному подходу. Результаты исследования имеют значение для совершенствования законодательства о киберпреступности и формирования профессиональных компетенций юристов в условиях технологической неопределенности.

Ключевые слова: научно-технический прогресс, киберпреступность, уголовное право, технологические риски, информационная безопасность, правовой регулятор, цифровая трансформация, адаптивное право.

E. V. Fokina
Candidate of Economic Sciences,
Rostov State University of Economics (RSUE),
branch in Yeysk, Krasnodar Krai

Criminal-law limits in regulating side effects of scientific and technological development

Abstract. Scientific and technological progress demonstrates exponential dynamics of development, outpacing the adaptive capacity of legal institutions. The article analyses the phenomenon of "side effects" of technological progress as a source of cybercrime, identifies structural limits of criminal legislation in managing technological risks, and substantiates the transition from a repressive model to a risk-oriented approach. The research results are significant for improving cybercrime legislation and developing professional competencies of lawyers in conditions of technological uncertainty.

Keywords: scientific and technological progress, cybercrime, criminal law, technological risks, information security, legal regulation, digital transformation, adaptive law.

Введение

Современный этап развития человечества характеризуется сингулярным ускорением технологических трансформаций. Согласно данным Всемирного экономического форума (2025 г.), период адаптации общества к новым технологиям сократился с 50 лет (эпоха промышленной революции) до 2–3 лет в цифровую эпоху. Одновременно наблюдается рост киберпреступности на 240 % за пятилетний период, что свидетельствует о формировании устойчивого дисбаланса между скоростью технологических инноваций и возможностями правовой системы.

Особую остроту проблема приобретает в контексте трансформации объекта уголовно-правовой охраны. Если в индустриальную эпоху право защищало преимущественно материальные ценности (собственность, телесная неприкосновенность), то в цифровую эпоху объектом посягательства становятся нематериальные блага: конфиденциальность данных [1], целостность алгоритмов, доступность информационных систем. При этом классические конструкции уголовного права – субъект, субъективная сторона, объективная сторона, объект – размываются в условиях автономного функционирования ИИ-систем и децентрализованных цифровых экосистем.

Актуальность исследования обусловлена тремя факторами:

1. Нормативным пробелом: 68 % дел о киберпреступлениях в Российской Федерации [7] содержат споры о квалификации из-за отсутствия четких критериев отграничения технологических рисков от преступных проявлений.

2. Глобальным дисбалансом: национальные правовые системы не способны эффективно регулировать трансграничные цифровые процессы, что создает «зоны правового вакуума».

3. Профессиональным дефицитом: формирование юридических кадров происходит в условиях устаревания учебных программ относительно темпов технологических изменений.

Обзор литературы

Проблематика взаимодействия права и технологий получила отражение в трудах отечественных и зарубежных исследователей, однако комплексный анализ диалектики «прогресс – побочные эффекты – правовая реакция» остается недостаточно разработанным.

В отечественной юридической науке традиционно доминирует технократический подход. Работы И.Г. Смирнова [3] и М.А. Федотовой [2] подробно анализируют составы преступлений в сфере компьютерной информации, но ограничиваются формально-догматическим уровнем, не затрагивая философских основ правового регулирования технологий.

Зарубежные исследователи [5, 6] акцентируют внимание на этических аспектах цифровой трансформации, но их подходы носят преимущественно дескриптивный характер и слабо увязаны с инструментами уголовно-правового воздействия. Концепция «регуляторных песочниц» (regulatory sandboxes), разработанная в рамках

ЕС (Digital Services Act, 2023), представляет практический интерес, но не адаптирована к российской правовой системе с ее акцентом на запретительные методы регулирования.

Критический анализ литературы позволяет выделить два нерешенных вопроса:

1. Как соотнести принцип технологической нейтральности права с необходимостью предотвращения криминальных последствий технологий?

2. Какие инструменты уголовного права эффективны для управления рисками при сохранении инновационного потенциала?

Данная статья направлена на заполнение указанных пробелов через разработку концепции адаптивного уголовного права.

Основная часть

Под побочными эффектами научно-технического прогресса в уголовно-правовом контексте понимаются общественно опасные последствия технологических инноваций, не являющиеся прямой целью их создания, но закономерно возникающие в процессе эксплуатации.

Выделяются три уровня их проявления.

Уровень первый – технический. Возникает из-за неизбежного несовершенства технологических решений. Пример: уязвимости в протоколах передачи данных, которые изначально не были заложены разработчиками, но позволяют осуществлять несанкционированный доступ. Согласно статистике ENISA [4], 73% инцидентов кибербезопасности связаны именно с техническими побочными эффектами, а не с умышленными атаками.

Уровень второй – социальный. Обусловлен адаптацией технологий к криминальным целям в процессе их массового распространения. Классический пример – мессенджеры, созданные для коммуникации, но ставшие инструментом фишинга и распространения вредоносного ПО. Здесь ключевую роль играет эффект «двойного назначения»: одна и та же технология служит как легальным, так и преступным целям.

Уровень третий – системный. Проявляется на стыке технологий и институтов. Пример: алгоритмические системы кредитного скоринга, формально нейтральные, но воспроизводящие социальную дискриминацию из-за предвзятости обучающих данных. В деле № 2-4567/2024 банк был привлечен к ответственности по ст. 136 УК РФ за дискриминацию по признаку места жительства, хотя разработчики ИИ не закладывали дискриминационные критерии сознательно.

Анализ практики применения гл. 28 УК РФ позволяет выделить четыре структурных предела уголовного права в регулировании технологий:

Предел первый – технологическая нейтральность. Уголовное право не может запретить технологию как таковую, поскольку любая технология потенциально двойного назначения. Попытки прямого запрета (например, законопроект о запрете мессенджеров без передачи ключей шифрования, 2022 г.) неизбежно сталкиваются с

конституционными ограничениями (ст. 23–24 Конституции Российской Федерации) и технической неосуществимостью.

Предел второй – эффект «водяной кровати». Подавление одного вектора киберпреступности приводит к трансформации угрозы в иной формат. Так, ужесточение ответственности за фишинг (Федеральный закон от 24.07.2023 № 327-ФЗ) привело к росту атак через децентрализованные приложения на блокчейне – сектор, слабо охваченный действующим законодательством (рост на 180% в 2024–2025 гг.).

Предел третий – глобальная асимметрия юрисдикций. Национальное уголовное право бессильно против преступлений, инфраструктура которых расположена в юрисдикциях с иным правовым режимом. Согласно данным Интерпола (2025), только 12% киберпреступлений с трансграничным компонентом завершаются вынесением приговора.

Предел четвертый – инновационный парадокс. Чрезмерное уголовно-правовое регулирование подавляет легальные инновации. Пример: запрет на анонимные криптотранзакции в ряде стран привел к оттоку блокчейн-стартапов в юрисдикции с более гибким регулированием, что ослабило позиции национальных экономик в цифровой конкуренции.

На основе выявленных пределов предлагается переход к модели «адаптивного уголовного права», основанной на трех принципах:

Принцип первый – риск-ориентированность. Вместо запрета опасных технологий – регулирование их применения через обязательную оценку рисков на этапе разработки. С 2025 г. в России введена обязательная «этическая экспертиза» ИИ-систем в критической инфраструктуре. Предлагается распространить этот подход на все технологии с высоким криминальным потенциалом через институт предварительного правового заключения.

Принцип второй – многоуровневая ответственность. В условиях размытости субъекта преступления (особенно при участии ИИ) необходимо дифференцировать ответственность участников технологической цепочки:

– разработчик – за умышленное создание уязвимостей;

– оператор – за халатность при эксплуатации;

– владелец данных – за нарушение требований защиты.

Такой подход закреплен в ст. 274.1 УК РФ (новая редакция 2025 г.), но требует развития в судебной практике.

Принцип третий – регуляторные песочницы. Создание контролируемых сред для тестирования технологий без применения репрессивных мер при соблюдении условий безопасности. Опыт Банка России (песочница для финтех-проектов, 2024 г.) демонстрирует снижение числа правонарушений на 40% при одновременном росте инновационной активности.

Заключение

Таким образом, научно-технический прогресс неизбежно порождает побочные эффекты, часть из которых трансформируется в киберпреступность. Уголовное право не в состоянии и не должно стремиться к полному устранению этих эффектов – это противоречит самой природе инновационного развития. Однако право может и должно создавать условия для минимизации общественно опасных последствий через переход от запретительной модели к риск-ориентированному управлению.

Ключевой вывод исследования: эффективность уголовно-правового регулирования в цифровую эпоху определяется не жесткостью санкций, а способностью правовой системы адаптироваться к технологическим изменениям без утраты защитной функции. Концепция адаптивного уголовного права, основанная на принципах риск-ориентированности, многоуровневой ответственности и регуляторных инноваций, представляет собой баланс между безопасностью и свободой – фундаментальный императив правового государства в эпоху цифровой трансформации.

Список литературы

1. Вольдимарова Н.Г. Проблемы регламентации уголовной ответственности за незаконные получение и разглашение коммерческой, налоговой и банковской тайны // Безопасность бизнеса. 2021. № 3. С. 34-39.

2. Информационное право: учебник для вузов / под ред. М.А. Федотова. – 4-е изд., перераб. и доп. М.: Юрайт, 2026. 855 с.

3. Смирнов И.Г. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ: монография. – М.: Юрлитинформ, 2016. 306 с.

4. ENISA. Threat Landscape 2025 // European Union Agency for Cybersecurity. 2025. URL: https://www.enisa.europa.eu/publications/threat-landscape-2025 (дата обращения: 05.09.2025)

5. Schneier B. A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back. W. W. Norton & Company, 2023. 304 p.

6. Zuboff Sh. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, 2019. 704 p.

7. Статистические данные Генеральной прокуратуры Российской Федерации. URL: https://epp.genproc.gov.ru/ru/gprf/activity/statistics/ (дата обращения: 05.09.2025)

УДК 373.71

А. Д. Фрасов,
аспирант,
Ульяновский государственный университет

Основные тенденция роста киберпреступлений

Аннотация. Статья посвящена исследованию тенденции роста преступности в киберпространстве. Целью статьи является выявление приоритетных направлений подходов в борьбе с киберпреступностью. Основная задача исследования заключается в выявлении факторов и условий, оказывающих влияние на рост киберпреступлений. В процессе исследования были применены методы логического, общенаучного, правового, статистического и сравнительного анализа, которые позволили обеспечить достоверность анализа и обоснованность полученных выводов. В результате исследования выявлено, что на рост киберпреступлений влияет как социальная транзитивность, а именно разобщенность в семьях, что позволяет контролировать действия людей, наиболее подверженных мошенническим атакам, так и цифровизация, в том числе и развитие информационно-коммуникационных технологий, оказывающих влияние не только на интенсивность и объемы продвижения информации, но и на структуру денежной массы, а именно рост доли безналичных денежных средств.

Ключевые слова: мошеннические атаки, общественная опасность, киберпреступления, жертвы киберхищений, электронные средства платежа

A. D. Frasov,
Postgraduate Student, Ulyanovsk State University

The main trends in the growth of cybercrime

Abstract. The article is devoted to the study of the trend of the growth of crime in the cyber space. The purpose of the article is to identify the priority directions of approaches in the fight against cybercrime. The main objective of the study is to identify the factors and conditions that influence the growth of cybercrime. In the process of research, methods of logical, general scientific, legal, statistical and comparative analysis were applied, which allowed to ensure the reliability of the analysis and the validity of the conclusions obtained. The study revealed that the growth of cybercrimes is influenced by both social transitivity, namely, the disunity within families, which allows for the control of the actions of individuals who are most susceptible to fraudulent attacks, and digitalization, including the development of information and communication technologies, which affect not only the intensity and volume of information dissemination, but also the structure of the money supply, namely, the disunity in families, which allows for the control of the actions of people who are most susceptible to fraudulent attacks, as well as digitalization, including the development of information and communication technologies, which affect not only the intensity and volume

of information promotion, but also the structure of the money supply, namely, the increase in the share of non-cash funds.

Keywords: fraudulent attacks, public danger, cybercrimes, victims of cyberthefts, electronic means of payment

Введение. На сегодняшний день состояние киберхищений как в мире, так и в Российской Федерации неизменно растет.

Основная часть. Количество зарегистрированных уголовно наказуемых деяний, совершенных с использованием информационно-коммуникационных технологий, возросло на 13,1% и составило 765 400 преступлений, с соответствующей долей 40% от общего числа преступлений [1]. Стоит отметить, что общий ущерб от киберпреступлений за 2024 год составил 168 млрд. рублей.

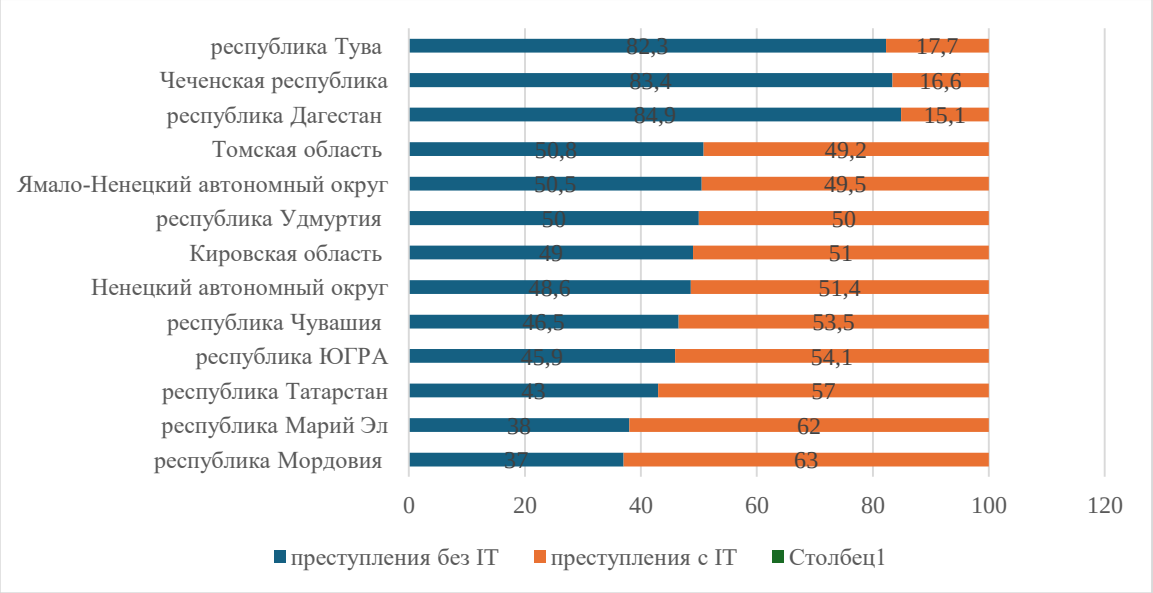

Рис. 1. Региональная специфика структуры преступлений с использованием ИТ (по состоянию в 2024 г.) [2]

Стоит отметить, что статистика киберхищений неоднородна по регионам Российской Федерации. К примеру, в данный момент имеется тенденция, по которой люди из южных регионов России менее подвержены мошенническим интернет-атакам, чем жители центральных, и северо-восточных регионов. Такие тезисы легко подтверждаются статистическими данными, по которым в 2024 году в региональном диапазоне преступления ИТ-направленности имеют показатели, представленные на рисунке 1:

Такая тенденция может быть обусловлена несколькими факторами:

- отсутствие разобщенности в семьях, что позволяет контролировать действия пожилых людей, наиболее подверженных мошенническим атакам;

-высокая осведомленности в отношении интернет-мошенников;

-минимальное количество безналичных денежных средств у населения.

Таким образом, ситуация с киберхищениями в Российской Федерации неоднородная, остается весьма острой и требует постоянных усилий в борьбе с указанным видом преступлений.

При рассмотрении динамики «киберхищений», стоит отметить любопытный фактор, который указывает на то, что рост числа подобных преступлений за последние 5 лет с 2020 по 2024 года нельзя назвать «резким», как в предыдущие годы, однако необходимо отметить существенное увеличение общей суммы ущерба, причиненного злоумышленниками в данном виде преступлений.

Динамика зарегистрированных киберпреступлений за период 2008г. по 2024гг. представлена на рисунке 2.

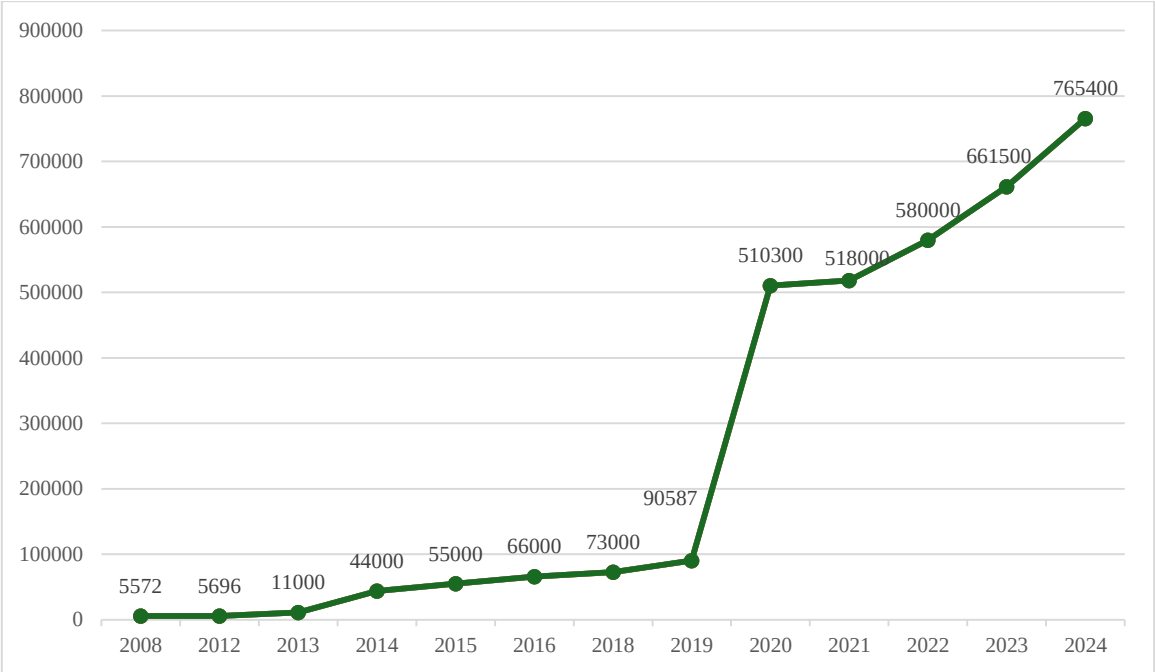

Рис. 2. Динамика зарегистрированных киберпреступлений за 2008- 2024 гг.

Динамика роста киберхищений отражает экспоненциальный рост случаев, а именно темп роста за последние 10 лет, с 5572 случаев в 2008 году до 764400 преступлений в 2024 году и составил 14 раз, а за последние 5 лет – 8,5 раз, с 90587 преступлений в 2019 году. Резкий взлет произошел в период 2019-2020 года, в пандемийный период.

В 2024 году рост количества «киберхищений» на территории Российской Федерации составил около 15% в сравнении с предыдущим годом. Однако, стоит отметить, что общий ущерб от указанного вида преступлений составил примерно 168 млрд. рублей. Учитывая, что количество зарегистрированных преступлений подобного характера в 2024 году составило 765 400 случаев, то при расчетах получается, что средняя сумма каждого «киберхищения» около 219493 рублей.

В свою очередь ущерб от ИТ-преступлений в 2020 году составил примерно 81 млрд. рублей, а количество зарегистрированных преступлений составило 210493 эпизода. Соответственно средняя сума каждого «киберхищения» составляла 384 810 рублей.

Однако данные показатели нельзя назвать снижением роста «киберпреступлений», поскольку количество «киберпреступлений» значительно увеличилось, а платежеспособность жертв данных преступлений практически не изменилась, что указывает на высокую общественную опасность данного вида преступлений.

Также, рассматривая динамику «киберхищений», необходимо затронуть тот факт, что дистанционные хищения и мошенничества значительно преобладают. За 2024 год из 765400 зарегистрированных киберпреступлений 486000 случаев, то есть 64% - составили киберпреступления, относящиеся к дистанционным хищениям и интернет-мошенничеству. Структура киберхищений за 2024 год представлены на рисунке 1.3.2. По данным структуры очевидно, что доля мошенничества с использованием электронных средств платежа преобладает в общем количестве киберхищений, а именно (рисунок 3):

Рис. 3. Структура киберпреступлений в 2024 году

– основная доля приходится на мошенничество 37% (ст. 159, 159^3, 159^6 УК РФ);

– кражи, 30% (ст.158 УК РФ);

– немного меньше - преступления, связанные с незаконной организацией и проведением азартных игр, доля которых в общей совокупности составляет 33% (ст. 172^1 УК РФ);

– деяния по незаконному производству, сбыту (пересылкой наркотических средств, психотропных веществ), а также незаконным сбытом или пересылкой растений, содержащих наркотические средства или психотропные вещества (ст. 228^2 УК РФ);

– 1% в совокупности, - преступления по изготовлению порнографических материалов (ст. 242, 242^2, 242^2 УК РФ), призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганды терроризма (ст. 205^2 УК РФ);

– призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ).

Стоит указать, что большая часть указанных преступлений, относящихся к киберхищениям, были совершены с использованием методов социальной инженерии и психологического давления.

Уровень раскрываемости киберпреступлений остается одним из низких, не превышая 25%.

В 2024 году Банк России провел исследование, по результатам которого было выявлено, что каждый 3-й из 10 респондентов указал на то, что он сталкивался с интернет-мошенниками. Также было отмечено, что 9% опрошенных лишились денежных средств в ходе взаимодействия с интернет-мошенниками.

Исследование портрета потерпевшего в результате «киберхищения» позволит выявить следующие аспекты.

Исходя и пола жертвы, статистика такова, что в 2024 г. жертв от интернет-мошенников среди женщин 52,6%, а среди мужчин 47,4%.

Рассматривая географическое положение жертвы, можно сказать, что среди жителей города число жертв интернет-мошенников составило 74,4%, а среди сельских жителей всего 25,6%.

Исходя из возраста жертвы, можно рассмотреть следующие статистические показатели:

– 14-19 лет – 10,8%;

– 20-24 года – 9%;

– 25-44 года – 36,1%;

– 45-64 года – 27,5%;

– от 65 лет – 16,6%.

Касаемо уровня образования у жертв интернет-мошенников, можно выделить 3 категории: общее образование, среднее образование, высшее образование. Указанные категории жертв интернет-мошенников имеют следующие статистические данные:

– общее образование – 32,4%;

– среднее образование – 42,7%;

– высшее образование – 24,9%.

Структура жертв кибермошенников по уровню дохода демонстрирует следующий формат:

– с низким уровнем дохода – 27,3%;

– со средним уровнем дохода – 46,2%;

– с высоким уровнем дохода – 26,5%.

По данным проведенного статистического исследования следует резюмировать, что основными жертвами киберхищений в 2024 году стали работающие женщины со средним уровнем дохода в возрасте от 25-ти до 44-х лет со средним уровнем образования, проживающие в городе.

Заметим, что реальные показатели могут несколько отличаться от официальных сведений, в силу того, что не все жертвы обращаются в полицию по разным причинам: кому-то неловко выставить себя беспечным и обманутым, кто-то не располагает временем на обращения по случившемуся факту киберхищения, у кого-то убежденность в бесполезности обращения. Тем не менее, представленные данные указывают на значимые показатели общественной опасности киберхищений.

Заключение. Таким образом, уровень актуальности изучения вопросов применения и совершенствования уголовно-правовых мер борьбы с киберхищениями на сегодняшний день как нельзя высок.

Список литературы

1. Капинус О.С. Цифровизация преступности и уголовное право / О.С. Капинус // Baikal Research Journal. 2022. Т.13, №1.

2. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // Официальный сайт Министерства внутренних дел Российской Федерации.

УДК 343.9

Л. Р. Хайрутдинова,
старший преподаватель,
Казанский инновационный университет
имени В. Г. Тимирясова,
Набережночелнинский филиал

Использование блокчейн-технологий в противодействии коррупции: обзор опыта зарубежных стран

Аннотация. Блокчейн-технологии становятся эффективным инструментом в борьбе с коррупций благодаря своей прозрачности, неизменяемости и децентрализации данных, что позволяет снизить риски фальсификации информации и противодействовать коррупции. Международный опыт показывает, что интеграция блокчейн-технологий в государстве обеспечило защиту данных, уменьшило коррупционные риски при предоставлении государственных услуг.

Ключевые слова: блокчейн, коррупция, противодействие коррупции, преступность, международный опыт, цифровизация, защита данных

L.R. Khairutdinova,
Senior Lecturer,
Kazan Innovative University
named after V.G. Timiryasov,
Naberezhnye Chelny branch

The use of blockchain technology in countering corruption: a review of foreign countries' experience

Abstract. Blockchain platform is one of the necessary and effective tools in the fight against corruption, due to its transparency and decentralization of data. Analysis of the experience of foreign countries, points to the effectiveness of blockchain technologies in the provision of public services.

Keywords: blockchain, corruption, anti-corruption, crime, international experience, digitalization, data protection

Введение. Коррупция является глобальной проблемой и, следовательно, ее правильное определение и классификация имеет первоочередное значение. Учитывая значительный рост использования цифровых и мобильных технологий, использование цифровых инструментов в государственных информационных системах имеет решающее значение для эффективной антикоррупционной деятельности в органах государственной власти, вследствии низкой эффективности существующих методов с учетом стремительного развития цифровизации. Ряд исследователей различают

потенциал таких технологий. В качестве способа использования такого потенциала ряд стран начали предлагать цифровые инициативы по борьбе с коррупцией, как часть усилий электронного правительства по трансформации государственного управления и его отношений [5].

Основная часть. На примере Российской Федерации были введены новые «суперсервисы «Поступление в вуз онлайн» (позволяющий удаленно подать документы и дистанционно оформить зачисление в вузы), «Социальная поддержка онлайн» (дающая возможность возникновения прав на получение мер социальной поддержки), «Цифровое исполнительное производство» (позволяющий проконтролировать ход исполнительногопроизводства и подать онлайн ходатайство без посещения судебных приставов), «Трудовые отношения онлайн», «Оформление европротокола онлайн», «Пенсия онлайн», «Онлайн-помощь при инвалидности». В рамках реализации программы «Цифровая экономика Российской Федерации» 11 апреля 2022 г. Правительством Российской Федерации была принята Концепция перехода к предоставлению 24 часа в сутки 7 дней в неделю абсолютного большинства государственных и муниципальных услуг без необходимости личного присутствия граждан» [3. С. 71].

Цифровое противодействие коррупции относится к числу цифровых инструментов, используемых для борьбы с коррупцией. Необходима и типология коррупции, которая определяет виды цифровых антикоррупционных инструментов, которые могут определить, какие цифровые меры применить против конкретных форм коррупции или устранять конкретные условия, способствующие коррупции, в определенных областях, деятельности и процедурах в государственном управлении.

В качестве мер, используются: Интернет-обращение – используется для обобщения, анализа и представления информации общественности для обеспечения прозрачности.

- Цифровая карта для визуализации информации на официальных сайтах;

-Автоматизация, которая устраняет дискрецию государственных и муниципальных служащих, исключает посредников и сокращает бюрократию;

- Реализация блокчейн - технологий.

Блокчейн – это распределенная и децентрализованная база данных, которая обеспечивает прозрачность, неизменности и безопасность имеющихся на платформе записей. Такие свойства делают блокчейн -технологии современным инструментов в борьбе с коррупцией.

Преимущества заключаются в том, что все операции записываются в общедоступный реестр, позволяя контролировать действия государственных и муниципальных служащих и в том числе и должностных лиц коммерческих организаций в реальном времени без возможности скрыть или изменить данные другой датой. Соответственно это исключает фальсификацию и подделку документов, отчетов, финансовых операций.

Отдельно отсутствует единая точка контроля блокчейн технологии, что снижает коррупционный риск, поскольку данные будут храниться на множестве узлов и проверятся участниками сети.

По своим возможностям, «блокчейн является практически идеальной платформой для надежного и долгосрочного хранения информации, сочетающей невозможность произвольного изменения данных с прозрачностью произведенных транзакций, что позволяет активно использовать эту технологию в любых публичных реестрах, в первую очередь в государственных» [1. С. 34].

Так, например в Дании, «система блокчейн является эффективным инструментарием в процессе противодействия коррупции. Система блокчейн используется правоохранительными органами для надзора за корпорациями (организациями), правительствами и заинтересованными группами, вследствие чего разрушаются многие коррупционные связи. В Дании система блокчейн является одним из актуальных механизмов противодействия коррупции» [2].

В Грузии используется блокчейн для регистрации собственности и сделок с землей, что снизило фальсификацию и коррупционные риски.

Эстония активно внедряет блокчейн в государстенном управлении для защиты данных и прозрачности госуслуг (регистрация бизнеса, регулирование системы здравоохранения).

В ОАЭ стартовал национальный блокчейн-проект для цифровизации государственных услуг и контрактов, сокращая бюрократические процедуры и коррупционные риски.

Индия – реализует проекты с блокчейн-технологиями для прозрачности голосования и регистрации собственности и контроля по распределению социальных выплат.

Можно рассмотреть ряд платформ, основанных на блокчейн технологиях:

Provenance – платформа для отслеживания происхождения товаров, обеспечивает прозрачность цепочек поставок и исключает коррупционные схемы в логистике.

Bitfury Crystal – аналитический инструмент на основе блокчейна для отслеживания финансовых потоков и выявления коррупционных транзакций.

«Инновационный инструмент также предлагает запатентованную систему «оценки рисков», помогающую выявлять и отслеживать подозрительные действия. Crystal был разработан для использования правоохранительными органами, для установления реальных личностей объектов, совершающих подозрительные транзакции биткоинов, и определения взаимосвязей между преступными действиями, а также для использования финансовыми и другими учреждениями, участвующими в расследовании и предоставляющих юридическую экспертизу» [4].

Follow My Vote – проект электронного голосования на блокчейне, предотвращающий нарушения прав избирателей, незаконные манипуляции с результатами голосования.

Платформы используемы для закупок и тендеров, которые снижают коррупционные риски:

VEChain – обеспечивает прозрачность логистики и обратной связи по качеству продукции, что снижает коррупционные риски при госзакупках.

OpenProcurement – система на базе блокчейна для проведения открытых и прозрачных государственных закупок.

Эти результаты показывают, что в государственном секторе существуют различные цифровые инструменты борьбы с коррупцией. Однако существующие попытки их классификации не в полной мере охватывают различные формы коррупции, виды деятельности и коррупционные процедуры, сферы государственного сектора, в которых имеет место коррупция и условия, способствующие проявлению коррупции.

Следовательно, необходимо разработать более всеобъемлющую типологию цифровых средств борьбы с коррупцией, которая связывала бы цифровые инструменты борьбы с коррупцией с различными видами и формами коррупции.

Заключение. Правильная классификация природы коррупции имеет основополагающее значение для разработки цифровых технологий, учитывающих основные характеристики интересующего конкретного вида коррупции. Правильная классификация гарантирует, что технологический инструмент хорошо справляется с задачей сбора данных о нужном явлении, на которое нацелена технология цифровой борьбы с коррупцией.

Список литературы

1. Аносов А.В. Цифровые технологии в системе предупреждения коррупционной преступности // Уголовная политика России на современном этапе: состояние, тенденции, перспективы. Сборник научных трудов по материалам международной конференции (к 100-летию со дня рождения Н.А. Стручкова). Москва, 2022. С. 30-35.

2. Гумаров И. А., Фарахиев Д. М. Технология Blockchain как средство противодействия коррупции // Научный компонент. 2022. №1 (13). URL: https://cyberleninka.ru/article/n/tehnologiya-blockchain-kak-sredstvo-protivodeystviya-korruptsii (дата обращения: 03.09.2025).

3. Пономаренко Е.В. Новые возможности искусственного интеллекта в противодействии коррупции // В сборнике: Новеллы права, образования, экономики и управления . Сборник научных трудов по материалам X международной научно-практической конференции . Гатчина, 2025. С. 70-74.

4. Crystal – инструмент для расследования махинаций с криптовалютами // https://hightech.fm/2018/01/31/crystal.

5. Fredrick Mutungi. Digital Anti-Corruption Typology for Public Sector // East African Journal of Information Technology, Volume 6, Issue 1, 2023. P.45-65.

УДК 343.2/.7

С. А. Хамидуллин,
аспирант,
Казанский инновационный университет
имени В. Г. Тимирясова

Цифровые финансовые инструменты: природа и роль при совершении преступлений

Аннотация. В статье рассматриваются актуальные вопросы правового регулирования отдельных цифровых финансовых инструментов в контексте коррупционных правонарушений. Проводится анализ текущего состояния действующего законодательства по их регулированию и существующих точек зрения исследователей. Автором подчеркивается необходимость системной проработки законодательных положений по регулированию цифровых финансовых инструментов.

Ключевые слова: уголовное право, гражданское право, цифровые финансовые инструменты, цифровой финансовый актив, цифровой рубль, конфискация, антикоррупционное законодательство

S.A. Khamidullin,
postgraduate student,
Kazan Innovative University
named after V. G. Timiryasov

Digital financial instruments: nature and role in criminal activities

Abstract. The article examines topical issues of legal regulation of certain digital financial instruments in the context of corruption offences. It analyses the current state of existing legislation on their regulation and the existing views of researchers. The author emphasises the need for a systematic review of legislative provisions on the regulation of digital financial instruments.

Keywords: criminal law, civil law, digital financial instruments, digital financial assets, digital ruble, confiscation, anti-corruption legislation

Введение. На сегодняшний день информационные технологии являются неотъемлемой частью современной жизни общества. Автоматизация существующих общественных процессов позволяет значительно улучшить качество жизни современного человека. Благодаря цифровизации, люди получают доступ к огромному объему информации, что способствует повышению уровня образования, качества коммуникации и появлению инноваций, трансформируя привычные сферы жизни, такие как медицина, образование и экономика. В частности, развитие цифровых финансовых инструментов, интегрированных в информационные системы,

революционизирует экономическую сферу, предоставляя возможность использования указанных финансовых средств для обеспечения финансовой инклюзии и создания новых моделей инвестирования.

Основная часть. Современный этап развития финансовых технологий характеризуется стремительным внедрением цифровых финансовых инструментов, таких как криптовалюты, невзаимозаменяемые токены (NFT), цифровые финансовые активы, цифровой рубль и другие финансовые средства, что существенно трансформирует традиционные подходы к финансовым операциям. Эти технологии обеспечивают высокую скорость транзакций, снижение операционных издержек и расширение доступа к финансовым услугам. Однако их использование сопряжено с рисками для интересов общества и государства, поскольку они могут быть задействованы в совершении коррупционных правонарушений, отмывании денег и иной противоправной деятельности. Статья посвящена анализу природы цифровых финансовых инструментов, их роли в коррупционных схемах и проблемам правового регулирования, с акцентом на необходимость сбалансированного подхода, сочетающего стимулирование инноваций с обеспечением безопасности общества.

Современные цифровые финансовые инструменты представляют собой продукт эволюции финансовых технологий, интегрированных в цифровые экосистемы. Их отличительными чертами являются высокая скорость операций, снижение транзакционных издержек и доступность для широкого круга пользователей. Например, такие цифровые финансовые инструменты, как криптовалюты, основанные на технологии распределенного реестра, обеспечивают децентрализованный и анонимный характер транзакций, что делает их уникальными по сравнению с традиционными финансовыми средствами. Тем не менее, указанные преимущества имеют и обратную сторону. Отсутствие централизованного контроля и прозрачности создает условия для злоупотреблений, в частности, при совершении коррупционных правонарушений.

На основе анализа научных работ, опубликованных в периодических изданиях и сборниках, авторы пытаются обобщить ключевые проблемы и предложения по правовому регулированию цифровых финансовых инструментов, подчеркивая необходимость разработки сбалансированного подхода, который бы сочетал стимулирование инноваций с минимизацией рисков для экономики и общества.

Одним из главных вопросов остается неопределенность правового положения отдельных цифровых финансовых инструментов. Так, А.М. Мусатов отмечает, что в настоящее время в уголовном законе отсутствуют четкие критерии и определения преступлений, совершенных с использованием цифровых валют, что в результате может привести к сложностям при квалификации тех или иных общественно опасных деяний, совершенных с их использованием. По мнению автора, указанное обстоятельство не только затрудняет работу правоохранительных органов, но и создает

предпосылки для уклонения от ответственности лиц, использующих цифровые активы в противоправных целях [6].

А.В. Жуков в своем исследовании указывает на проблемы декларирования криптовалют государственными служащими, которые обусловлены отсутствием четкого правового статуса в законодательстве России, акцентируя внимание на том, что указанное финансовое средство может служить инструментом для сокрытия коррупционных правонарушений. Автор подчеркивает, что анонимность и децентрализованный характер указанного финансового инструмента делают его идеальным средством для обхода традиционных механизмов контроля, что особенно актуально в контексте антикоррупционного законодательства [2].

При этом, И.А. Лисовская и Н.Г. Трапезникова отмечают, что, несмотря на значительное количество исследований в данной области, в настоящий момент отсутствует системный подход в определении отдельных цифровых финансовых инструментов. Авторы подчеркивают, что существование разнообразных подходов к определению и классификации инструментов свидетельствует не только об их новизне, которая порождает трудности и многозначность интерпретаций, но и указывает на потребность в точной идентификации каждого из этих объектов правоотношений. По их мнению, отсутствие единого концептуального аппарата препятствует разработке эффективных мер их регулирования и контроля [5].

Вопросы также возникают в сфере правового регулирования цифрового рубля. И.В. Камбурова, анализируя в статье цифровой рубль в качестве финансового инструмента указывает на пересечение его функций с безналичными денежными средствами, подчеркивая, что на сегодняшний день нет четкого определения указанного средства платежа, что порождает правовую неопределенность в его применении. При этом автор акцентирует внимание на том, что отсутствие законодательно закрепленного статуса цифрового рубля усложняет его интеграцию в существующую финансовую систему и создает риски для обеспечения прозрачности операций [3].

По нашему мнению, представленные позиции являются обоснованными. Отсутствие системного подхода в определении правовой природы отдельных видов цифровых финансовых инструментов может вызвать определенные трудности их правового регулирования, квалификации связанных с ними правонарушений и обеспечении единообразной правоприменительной и судебной практики. Это, в свою очередь, создает условия для возникновения правовой неопределенности, которая затрудняет как деятельность участников рынка, стремящихся использовать данные инструменты в общественно полезных целях, так и работу правоохранительных органов, направленную на пресечение противоправных действий, включая коррупционные правонарушения.

Так, например, в соответствии с решением по делу № 8Г-38110/2023 от 26 декабря 2023 года, в котором Никулинский районный суд г. Москвы по уголовному

делу, возбужденному по ч.6 ст. 290 УК РФ, в отношении бывшего следователя Марата Тамбиева, постановил конфисковать цифровую валюту в виде «биткоинов», хранящуюся на аппаратном криптокошельке «Ledger Nano X» [9]. Однако на сегодняшний день предпринимаются попытки по разработке механизма изъятия цифровых валют в доход государства [7].

Кроме того, отсутствие четкого и унифицированного определения понятия «цифровые финансовые активы» в отечественном законодательстве остается одной из основных проблем правового регулирования. На текущий момент предпринимаются шаги для устранения этой неопределенности. Так, в марте 2025 года председатель Следственного комитета Российской Федерации (далее - СК РФ) А.И. Бастрыкин объявил о завершении совместной работы СК РФ и Министерства юстиции Российской Федерации над законопроектом о внесении изменений в действующее уголовное законодательство и признании цифровых валют имуществом. Согласно данным, опубликованным в открытых источниках, основными задачами законопроекта являются закрепление статуса цифровых валют как имущества, создание правовых оснований для наложения на них ареста, признания их в качестве вещественных доказательств, а также обеспечение возможности конфискации цифровых валют в доход государства [4]. В настоящий момент законопроект прошел рассмотрение в первом чтении.

Согласно содержанию законопроекта, в примечание к статье 104.1 Уголовного кодекса Российской Федерации (далее – УК РФ) вводится пункт 2, согласно которому *«цифровая валюта признается имуществом»* для целей уголовного закона. Вместе с тем место цифровой валюты в системе объектов гражданских прав, предусмотренных статьей 128 Гражданского кодекса Российской Федерации, по-прежнему не урегулировано [1]. В связи с этим, на практике возникает комплекс правовых неопределенностей, в частности, при определении предмета и способа конфискации в случаях, когда изъятие «в натуре» невозможно из-за отсутствия закрепленной методики денежной оценки цифровых финансовых инструментов, а также при обеспечении сохранности активов посредством перевода на адрес-идентификатор с одновременным соблюдением требований к надлежащей фиксации доказательственной информации.

Кроме того, в правовом регулировании оборота цифровых финансовых активов, в частности, цифровых финансовых валют, выявляется существенное противоречие. В соответствии с определением, приведенным в Федеральном законе от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», цифровая валюта признается одновременно средством платежа и объектом инвестирования, что предполагает ее многофункциональный характер. Однако статья 14 закона устанавливает запрет для юридических и физических лиц на принятие цифровой валюты в качестве платежного средства. Данное ограничение вступает в противоречие с декларируемым статусом цифровой валюты как средства платежа, что создает

правовую коллизию и препятствует ее полноценной интеграции в экономические процессы. Указанные несоответствия подчеркивают необходимость дальнейшей доработки нормативной базы для устранения коллизий и обеспечения согласованности правового режима цифровых финансовых инструментов.

Заключение. На сегодняшний день развитие цифровых финансовых инструментов достигло такого уровня, при котором их влияние на экономику и общество становится одновременно значительным и неоднозначным. Многочисленные и разнообразные пути проникновения цифровых технологий в повседневную жизнь в последние годы позволяют сделать вывод о том, что теперь «жизнь стала цифровой» [10. С. 637]. С одной стороны, они способствуют прогрессу, упрощению финансовых операций и расширению доступа к инвестиционным возможностям, с другой - создают новые вызовы для правовой системы, особенно в сфере уголовного права. Отсутствие четкого правового статуса, единообразных определений и системного подхода к регулированию этих инструментов приводит к пробелам в законодательстве, усложняет квалификацию преступлений и повышает риски их использования в противоправных целях, в том числе при совершении коррупционных правонарушений, что подчеркивает острую необходимость разработки комплексных мер, обеспечивающих баланс между развитием новых технологий и защитой общественных интересов.

Список литературы

1. Гражданский кодекс Российской Федерации (часть первая): Федеральный закон от 30.11.1994 № 51-ФЗ (в ред. по состоянию на 31.07.2025). URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 08.09.2025).

2. Жуков А.П. Правовые проблемы декларирования криптовалюты для гражданских и государственных служащих в РФ // Образование и право. 2025. С. 447-451.

3. Камбурова И.В. Сравнительный анализ цифрового рубля с другими формами национальной валюты // Аудиторские ведомости. 2025. № 1. С. 99-103.

4. Криптовалюту признают имуществом? Юристы прокомментировали инициативу СК. URL: https://www.rbc.ru/crypto/news/67dab74f9a79472be9903158?ysclid=m94dsv6ka6571373680 (дата обращения:01.09.2025).

5. Лисовская И. А., Трапезникова Н. Г. Цифровые финансовые инструменты: классификация, характеристика основных видов, подходы к отражению в финансовой отчетности // Бизнес. Образование. Право. 2025. № 1(70). С. 51-57. С. 447-451.

6. Мусатов А.М. Уголовно-правовая оценка экономических преступлений с использованием финансовых активов и цифровой валюты // Закон и право. 2024. № 12. С. 248-252.

7. Приставы готовятся к массовому аресту криптовалюты. URL: https://www.moscowtimes.ru/2025/04/02/pristavi-gotovyatsya-kmassovomu-arestu-kriptovalyuti-a159942 (дата обращения:01.09.2025).

8. Решение по делу № 8Г-38110/2023 от 26.12.2023. URL: https://reputation.su/sudrf/248367002?ysclid=m94eeaq4l9437752 (дата обращения:01.09.2025).

9. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (в ред. по состоянию на 01.09.2025). URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 08.09.2025).

10. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_358753/?ysclid=m94epp0hco256585198 (дата обращения:01.09.2025).

11. Спайропулос Ф. Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии // Journal of Digital Technologies and Law. 2024. Т. 2, № 3. С. 636-656. https://doi.org/10.21202/jdtl.2024.32. EDN: mqtnqg

УДК 343.3

С. А. Хлебунова,
кандидат юридических наук, старший преподаватель,
Челябинский государственный университет

Уголовно-правовой аспект использования цифровых технологий в организации незаконной миграции

Аннотация. В статье рассмотрена проблема уголовного наказания за преступления в сфере миграционных отношений, совершенных по средствам применения новых технологий информационно-телекоммуникационных сетей, в том числе сети «Интернета». Предлагается статьи 322, 322.2, 322.3 Уголовного кодекса Российской Федерации дополнить квалифицирующим признаком, как «совершенные с применением информационно-телекоммуникационных сетей, в том числе сети «Интернета». В качестве отягчающего обстоятельства за нанесение значительного вреда общественной и национальной безопасности страны внедрить состав преступления, предусмотренный статьей 322.4 «Совершение действий, предусмотренных статьями 322, 322.1, 322.2 и 322.3 Уголовного кодекса Российской Федерации путем незаконного использования и подключения к электронным порталам и сайтам государственных и муниципальных органов».

Ключевые слова: миграционные преступления, уголовная ответственность за миграционные преступления, организация незаконной миграции, преступления в сфере миграции

S.A. Khlebunova,
Candidate of Law, Senior Lecturer,
Chelyabinsk State University

The criminal-legal aspect of the use of digital technologies in the organization of illegal migration

Abstract. The article discusses the problem of criminal punishment for crimes in the field of migration relations committed by means of information and telecommunication networks, including the Internet. It is proposed to supplement the criminal legislation of the Russian Federation with a qualifying feature regarding Articles 322, 322.2, and 322.3 of the Criminal Code of the Russian Federation, "committing crimes using information and telecommunication networks, including the «Internet». As an aggravating circumstance for causing significant harm to the country's public and national security, introduce a new criminal offense under Article 322.4 of the «Criminal Code of the Russian Federation, which provides for the illegal use and connection to electronic portals and websites of state and municipal authorities».

Keywords: migration crimes, criminal liability for migration crimes, organization of illegal migration, migration crimes

Введение. В современном мире цифровые технологии активно используются в преступных целях. Набирают популярность преступления, связанные с нарушением миграционного законодательства Российской Федерации, совершение которых связано с применением информационно-телекоммуникационных сетей, в том числе сети «Интернета». Внедренная в российское законодательство уголовная ответственность за преступления в сфере миграции находится на стадии становления и не способна в полной мере регулировать преступления, совершенные с использованием цифровых технологий, поскольку не всегда возможно спрогнозировать какими новыми возможностями и способами воспользуются преступники. Ужесточение миграционной политики напрямую касается увеличения размера и срока санкций за преступления в миграционной сфере, а также введение нового квалификационного основания, предусматривающего уголовную ответственность за нарушение миграционного законодательства при использовании сайтов органов публичной власти.

Обсуждение. По итогам 2024 года результатов деятельности подразделений по вопросам миграции территориальных органов МВД России отмечается возросшее в 2 раза (с 1259 до 2490) число выявленных преступлений по статье 322.1 Уголовного кодекса Российской Федерации. Увеличился показатель выявленных и расследованных преступных деяний, связанных с фиктивной постановкой на учет иностранных граждан и лиц без гражданства по месту пребывания в России на 3,3% (36 110) по статье 322.3 Уголовного кодекса Российской Федерации [1]. За рассматриваемый период не представлено информации о преступлениях по статье 322.2 Уголовного кодекса Российской Федерации. Однако в первой половине 2025 года продолжается количественный рост преступлений по статье 322.1 Уголовного кодекса Российской Федерации на 7,2 % (с 1268 до 1359)[2].

За 2023–2024 год на сайте Судебной статистики Российской Федерации прослеживается динамика ежегодного увеличения преступлений по статьям 322.1, 322.2, 322.3 Уголовного кодекса Российской Федерации [3] (рис.1).

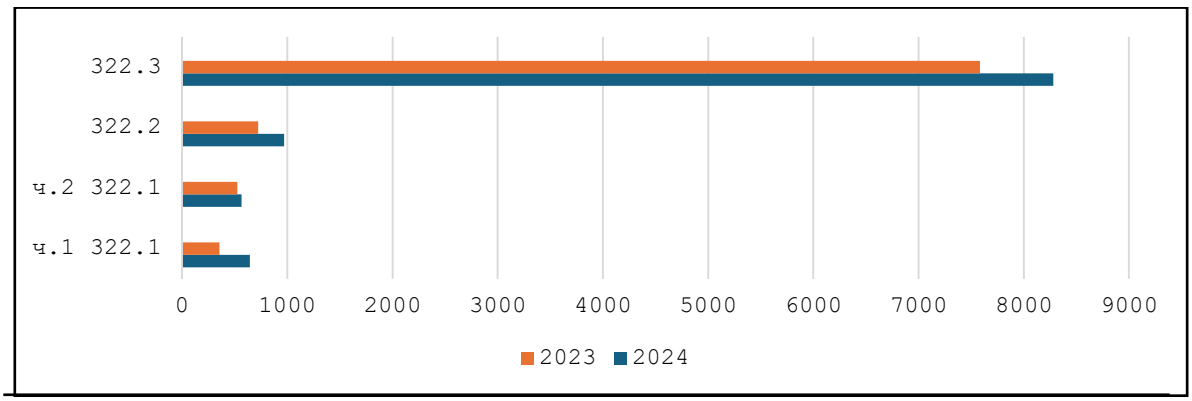

Рис. 1 Осуждено за преступления в сфере миграции в Российской Федерации за 2023-2024 года

Количество преступлений в сфере миграции не только из года в год увеличивается, но сопровождается внедрением новых способов по их организации и совершению. Преступники активно используют современные технологии для организации незаконной миграции, фиктивной постановки на миграционный учет и регистрации по месту жительства в жилых помещениях иностранцев и лиц без гражданства. Многие специалисты выражают озабоченность, что большой процент преступлений в сфере миграции в настоящее время совершается при помощи электронных мессенджеров, размещением фейковых сайтов по оказанию миграционных услуг, откровенным взломом государственных интернет-порталов [4;5]. Соглашаясь с мнением И. Р. Бегишева и В.В. Денисович следует «пересмотреть структуру объектов уголовно-правовой охраны и специфику привлечения лиц к уголовной ответственности, обладающих специальными познаниями в сфере продуктов достижения цифровых технологий, внести соответствующие изменения в структуру статей Особенной части Уголовного кодекса Российской Федерации» [6]. Так, в августе 2025 году «сотрудники Управления по борьбе с противоправным использованием информационно-коммуникационных технологий ГУ МВД России по г. Санкт-Петербургу и Ленинградской области задержали шестерых местных жителей, которые с 2023 года организовали незаконную миграцию для иностранных граждан используя аккаунты россиян на Едином портале государственных и муниципальных услуг» [7]. Несмотря на возросшее в целом количество преступлений, совершенных в цифровом пространстве официальные статистические данные правоохранительных органов, не содержат информацию о количественных показателях преступлений совершенных с использованием IT-технологий, а также относительно преступлений в сфере миграции.

Федеральным законом от 09.11.2024 № 383-ФЗ приняты меры повышающие уголовную ответственность по всем статьям 322.1, 322.2, 322.3 Уголовного кодекса Российской Федерации, в них введены новые квалификационные признаки и увеличен предельный срок наказания. По части 1 статьи 322.1 «Организация незаконной миграции» Уголовного кодекса Российской Федерации санкции увеличены с трех до пяти лет со штрафом до 500 тысяч рублей; по части 2 статьи 322.1 Уголовного кодекса Российской Федерации срок наказания достигает до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до 5 лет либо без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 7 лет или без такового» [8]. Введена часть 3 статьи 322.1 в случае совершения «деяний первой и второй частей данной статьи, совершенные организованной группой или в целях совершения тяжких или особо тяжких преступлений на территории Российской

Федерации, налагается санкция по лишению свободы на срок от восьми до пятнадцати лет со штрафом в размере от трех миллионов до пяти миллионов рублей или в размере заработной платы или иного дохода осужденного за период от трех до пяти лет либо без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до десяти лет или без такового» [8]. Несмотря на ужесточение санкций за миграционные преступления, только в части второй статьи 322.1 Уголовного кодекса Российской Федерации добавлен квалификационный признак, позволяющий привлекать к уголовной ответственности «с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Ужесточение уголовной ответственности за преступления в сфере миграции необходимый и своевременный шаг по регулировании миграционных отношений, которые непосредственно связаны с экономическим развитием Российской Федерации и ее национальной безопасности. Работающие нелегально мигранты не платят подоходный налог, а их работодатели не отчисляют за них взносы в социальный и медицинские фонды. В результате бюджеты разных публичных уровней не дополучают налоги для развития других социальных программ. С другой стороны, работодатели, нанимая нелегалов для работы экономят на оплате их труда и создают не конкурентные условия для легальных работников, ухудшают их трудовые условия. Подобные действия приводят к процветанию так называемой теневой экономики и подпитывают коррупцию служащих государственного и муниципального сектора. Появляются организованные преступные группы, развивается криминализация сферы миграции. В свою очередь повышенный уровень нелегальной миграции приводит к снижению международного имиджа государства в целом и отпугивают в привлекательности крупных иностранных инвесторов готовых вкладываться в развитие экономики.

К другой значимой проблеме, относится обеспечение национальной безопасности Российской Федерации. Организованные преступные группы реализующие каналы нелегальной миграции, обходят установленные законом процедуры и пограничный контроль, тем самым непосредственно нарушая государственный суверенитет, а также создают условия для проникновения на территорию нашего государства радикально настроенных людей, которые своими действиями будут создавать условия для совершения террористических актов, разжигать межнациональную и религиозную вражду в обществе. Провоцируется рост социальной напряженности, межнациональных конфликтов и насаждаются ксенофобские настроения в среде местного населения, что создает угрозу общественному прядку и национальной безопасности страны в целом.

Преступления совершенные в сфере миграции представляют собой серьезную опасность, которая подрывает основы правового государства, наносит бюджету финансовый ущерб, создает несправедливую конкуренцию, тормозит экономическое развитие страны, влияет на территориальную целостность страны, ослабляется контроль государственных институтов.

Следуя государственной политикой по ужесточению миграционного законодательства за совершение преступлений в сфере миграции и учитывая значимость этой сферы для государства представляется возможным выделить статьи 322, 322.1, 322.2 и 322.3 Уголовного кодекса Российской Федерации Особенной части Уголовного кодекса Российской Федерации в отдельную группу преступлений, совершаемых в сфере миграции. С одной сторон, обособление группы преступлений в сфере нарушения миграционного законодательства подчеркнет их общественное и государственное значение, а также отделит состав этих преступлений от подобных. С дугой стороны, применение современных цифровых технологий для совершения преступлений в сфере миграции вероятно только увеличатся. Следовательно, потребуется введение новых составов, предусматривающих использование цифровых технологий, поскольку сегодня трудно спрогнозировать как они будут применяться преступниками. Отсутствие квалификационных признаков преступлений связанных с применением цифровых технологий не позволит в судебном прядке, их правомерно квалифицировать и соразмерно определять степень наказания.

Заключение. Несмотря на принимаемые государством меры безопасности остаются риски несанкционированного проникновения и преступного использования государственных и муниципальных порталов, содержащих персональные данные российских граждан. Видится целесообразным расширить квалифицирующие признаки статей 322, 322.2, 322.3 Уголовного кодекса Российской Федерации, добавив в каждую из них «использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». Внедрение данного квалифицированного признаки позволит учитывать характер и степень общественной опасности миграционных преступлений и выступать отягчающим видом для определения судами наказания. Предлагается ввести в уголовный закон России дополнительный состав преступления – совершение действий, предусмотренных статями 322, 322.1, 322.2 и 322.3 путем незаконного использования и подключения к электронным порталам и сайтам государственных и муниципальных органов (статья 322.4 УК РФ).

Суровость наказания обусловлена совершением преступных действий, связанных с несанкционированным обходом защитных систем государственных и муниципальных цифровых ресурсов. Подобные преступления создают угрозу общественной и национальной безопасности Российской Федерации. Кроме того, введение уголовной ответственности и максимально суровое наказания за миграционные преступления, совершенные с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» выступит мерой сдерживания для совершения подобных правонарушений.

Список литературы

1. Аналитическая справка о результатах деятельности подразделений по вопросам миграции территориальных органов МВД России за январь-декабрь 2024

года. Статистика и аналитика. Официальный сайт МВД России // URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics/migracionnaya/item/63022223/ (дата обращения 18.08.2025).

2. Аналитическая справка о результатах деятельности подразделений по вопросам миграции территориальных органов МВД России за январь-июнь 2025 года. Статистика и аналитика. Официальный сайт МВД России // URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics/migracionnaya/item/68790619/ (дата обращения 18.08.2025).

3. Судебная статистика РФ https://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 (дата обращения 18.08.2025).

4. Яровая И.А. Заместитель Председателя Государственной Думы, руководитель межфракционной парламентской комиссии по вопросам миграционной политики И.А. Яровая, при комментировании единогласного принятие законопроекта о введении внесудебной блокировки интернет-ресурсов, содержащих предложения незаконных услуг для мигрантов, озвучила, что «треть преступлений, касающихся организации нелегальной миграции совершается с использованием IT-технологий» // URL: https://xn--80ad9ah8ee.xn--p1ai/news/interesy-semey/irina-yarovaya-otsechenie-bolshogo-obyema-kommunikatsiy-vazhnoe-reshenie-v-borbe-s-organizovannoy-ne/?ysclid=meh3flp4k2920298347 (дата обращения 18.08.2025).

5. Голуб Я.О., Денисов А. операционный директор «Рейтинга Рунета» Анатолий Денисов говорит, что «процент теневых цифровых услуг может доходить до 50% и даже больше» и директор сервиса мониторинга персонала «Инсайдер», руководитель digital-агентства Intec Ярослав Голуб полагает, что «показатель значительно выше – вплоть до 80–90% преступлений в сфере миграции с использованием IT-технологий» // URL: https://www.dp.ru/a/2024/11/06/migranti-izmatrici-vlasti (дата обращения 18.08.2025).

6. Бегишев, И. Р. Метавселенные в уголовно-правовом измерении / И. Р. Бегишев, В. В. Денисович // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции : в 6 т., Казань, 22 сентября 2023 года. Казань: Познание, 2023. С. 40-44. EDN QJOYKU. (дата обращения 18.08.2025).

7. Официальный сайт МВД России, раздел «Новости» https://xn--b1aew.xn--p1ai/news/item/68485908/ (дата обращения 18.08.2025).

8. Часть 2 статьи 322.1 Уголовного кодекса Российской Федерации // СПС «Консультант плюс» (дата обращения 18.08.2025).

УДК 343:004

В. Н. Швороб,
соискатель, преподаватель,
филиал Красноярского государственного аграрного университета,
С. М. Курбатова,
доктор юридических наук, профессор,
Сибирский федеральный университет,
Красноярский государственный аграрный университет

Цифровые технологии и право: некоторые аспекты цифровизации уголовного судопроизводства

Аннотация. В статье рассмотрены общие тенденции внедрения цифровых технологий в право и непосредственно в уголовный процесс, а также необходимость их правовой регламентации. Раскрываются проблемные аспекты понятийного аппарата в сфере цифровизации права и правосудия. Также анализируются проблемы, связанные с ними риски правового регулирования уже внедренных технологий в уголовное судопроизводство, с целью их устранения и совершенствования процесса для повышения эффективности правоприменения.

Ключевые слова. Цифровизация, цифровые технологии, цифровое право, правосудие, судопроизводство, электронный документооборот, видеоконференцсвязь

V. N. Shvorob,
Applicant, Lecturer,
Branch Krasnoyarsk State Agrarian University,
S. M. Kurbatova,
Doctor of Law, Professor,
Siberian Federal University,
Krasnoyarsk State Agrarian University

Digital technology and law: some aspects of digitalization of criminal proceedings

Abstract. The article examines the general trends of the introduction of digital technologies in law and in the criminal process, as well as the need for their legal regulation. It reveals the problematic aspects of the conceptual framework in the field of digitalization of law and justice. The article also analyzes the problems and risks associated with the legal regulation of already implemented technologies in criminal proceedings, in order to eliminate them and improve the process in order to increase the effectiveness of law enforcement.

Keywords. Digitalization, digital technologies, digital law, justice, legal proceedings, generations, electronic document management, and video conferencing

Введение. История развития человечества знает много переломных моментов, играющих роль в формировании современного государства и общества. Чаще катализатором подобных событий является научно-технический и технологический прогресс, желание человека ускорить решаемые профессиональные задачи и упростить алгоритм совершаемых действий.

Актуальность темы цифровых технологий в российском правовом пространстве обусловлена тем, что наряду с новаторскими достижениями их использования в правовой сфере могут возникнуть риски и проблемы правового регулирования, связанные с доступом к правосудию участников процесса, так и процессуально-организационного характера. Вместе с тем, «поголовная» цифровизация общества идет по нарастающей, и отсутствие правового регулирования и придания законных оснований не остановит распространение цифровых технологий, а лишь может их притормозить.

Основная часть. В настоящее время действительность отражает развитие общества, ведущее к расширению круга общественных отношений, в том числе посредством использования современных (электронных, информационных, цифровых) технологий. Появление новых общественных связей, связанных с цифровизацией общества, обуславливает необходимость принятия государством мер к их правовому урегулированию, что стимулирует законодательную деятельность на введение новых регуляторов складывающихся общественных отношений, а также по закреплению на законодательном уровне внедрения современных технологий в деятельность государственных органов, представленных законодательной, исполнительной и судебной властью.

Так, по мнению авторов Н.Г. Маськовой и А.А. Хажгериевой, «в современном мире цифровые медиатехнологии становятся ключевой коммуникационной платформой. Они информируют аудиторию о происходящих событиях и явлениях в стране и в мире, формируют взгляды на важные социально-экономические и политические проблемы, а также являются инструментом выражениях общественных настроений и мнений. Так цифровые медиаплатформы для социума более важное значение, чем традиционные источники получения информации – СМИ. Медиа-платформы создают медиапространство, в котором реализуется множество процессов развития личности: саморазвитие, самореализация, социализация, адаптация к действующей социально-экономической и политической системам. В условиях появления социальных медиа-распространение получает групповая коммуникация и медиа-потребление» [6].

Новые поколения все больше углубляются в цифровые технологии и интернет-коммуникации, и свою жизнь уже не представляют без «гаджетов» и «Интернета».

Исследования поведения современных участников общественных отношений показали, что «цифровая трансформация затрагивает представителей всех поколений, оказывая влияние на формирование и изменение их ценностей, совершаемые покупки

и получаемую информацию. При этом, поколение людей, родившихся после 1994 года, вырастает и воспитывается в среде, где привычными составляющими повседневной жизни наряду с традиционными медиа становятся социальные сети, высокоскоростной интернет, мгновенный обмен информацией, беспроводные сети, планшеты, компьютеры. Традиционные способы познания мира, используемые представителями прошлых поколений, сменяются на оперативное и легкодоступное получение информации из гаджетов и мобильных приложений смартфонов. Эти факторы оказывают прямое воздействие на алгоритмы поведения новых поколений, особенности восприятия информации и культуру медиапотребления» [6]. Следовательно, для поколений, о которых выше идет речь, является естественным и удобным взаимодействие, как между собой, так и с государством и его исполнительными органами, посредством электронно-цифровых средств коммуникации в информационно-телекоммуникационной сети, с применением соответствующих приложений на различных интернет-платформах.

Ввиду глобальных изменений в сфере общественных отношений, связанных с цифровыми технологиями, на повестке государственного регулирования остро стоят вопросы, связанные с «цифровизацией», «цифровым правом» и, как следствие, «цифровым правосудием».

Вследствие чего Президент Российской Федерации, понимая проблему, ставит перед государственными органами соответствующие задачи. Так, Указом Президента РФ «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» [8] на государственном уровне установлены национальные цели развития Российской Федерации в обозначенные в указе периоды, в числе которых определены технологическое лидерство и цифровая трансформация государственного и муниципального управления. В силу чего определено разработать с использованием единой цифровой картографической основы Российской Федерации и утвердить комплексный план развития транспортной, энергетической, телекоммуникационной, социальной и иной инфраструктуры на период до 2036 года, необходимых для реализации национальных целей. Установив целевые задачи, выполнение которых характеризует достижение национальных целей, а именно достижение к 2030 году «цифровой зрелости» государственного и муниципального управления, ключевых отраслей экономики и социальной сферы, предполагающей автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта (п.п. а, п. 8 Указа № 309).

Многие ученные и исследователи в области права, экономики и образования отмечают с точки зрения применения цифровизации, в том числе в правовой сфере, отсутствие понятийного аппарата затрагиваемой темы, следовательно, возникающие

проблемы подходов и методов регулирования уже имеющих место быть общественных отношений в данной сфере.

По мнению многих авторов, в настоящее время понимание правовой природы и наиболее точное определение термина дано в учебном пособии «Цифровое право» под общей редакцией В.В. Блажеева и М.А. Егоровой. Так, авторами главы 1 указанного пособия В.С. Белых и М.А. Егоровой дано следующее понятие, «цифровое право – система общеобязательных, формально определенных, гарантированных государством правил поведения, которая складывается в области применения или с помощью применения цифровых технологий и регулирует отношения, возникающие в связи с использованием цифровых данных и применением цифровых технологий. С точки зрения системного подхода, цифровое право сегодня это комплексный институт права, объединяющий правовые нормы, регулирующие отношения, возникающие в связи с приобретением, осуществлением и отчуждением цифровых прав, а также с применением цифровых технологий физическими и юридическими лицами» [12].

Российское законодательство все более адаптируется к широкому использованию цифровых технологий. Цифровое право формируется цифровыми операциями (в том числе коммерческими) и профессиональным взаимодействием, построенным на основе цифровых способов, подходов и средств за счет использования цифровых технологий, в том числе сетевых, информационно-телекоммуникационных и иных IT-технологий [7].

В этих условиях процесс всеобщей цифровизации не мог не затронуть такую важную сферу государственной деятельности, как осуществление правосудия. В связи с этим возник и в последние годы и активно используются такие термины, как «электронное» или «цифровое» правосудие, в содержании которого ученные, судьи и граждане вовлеченные в процесс судопроизводства, вкладывают иногда разный смысл [13].

При всем разнообразии мнений об определении термина «электронное правосудие» (цифровое правосудие), как верно замечено И.И. Шереметьевым, наиболее полно это понятие раскрыто бывшим председателем Арбитражного суда г.Москвы С.Ю. Чучей [13], с чем нельзя не согласиться, поскольку было предложено «под электронным правосудием, отправляемым российскими судами, понимать деятельность судов по разрешению дел, отнесенных к их компетенции, с использованием информационно-коммуникационных технологий и систем, в том числе обеспечивающих электронный документооборот, формирование электронных дел и их архивов, с открытым доступом в сети «Интернет» об информации о ходе и итогах рассмотрения судебных дел» [14].

Учитывая многочисленные публикации за последнее десятилетие по данной теме ученных теоретиков и практиков процессуалистов о цифровизации права в общем и правосудия в частности, о пределах его внедрения, исследования проводились по большому счету по двум направлениям: в частности, внедрение цифровизации,

ограничившись «машиночитаемым правом» [10, 11] на основе «Концепции развития технологий машиночитаемого права», утвержденной Правительственной комиссией [4], или же с применением технологий на основе искусственного интеллекта [1, 3] в связи с принятым Указом Президента Российской Федерации № 309 [8] на основе постановления Правительства Российской Федерации «О Центре развития искусственного интеллекта при Правительстве РФ» [9].

Кроме того, на основании «Концепции информатизации Верховного Суда Российской Федерации» утвержденной приказом Председателя ВС РФ [5], установлены основные цели развитие судебной системы с использованием современных информационных технологий, положения которой направлены на совершенствование судопроизводства, в том числе посредством дистанционного ознакомления, уведомления и участия, обеспечение открытости и доступности правосудия, формирование открытых сведений о судебной системе реализацию требований информационной безопасности.

Однако на современном этапе развития уголовного процесса, основные модификации закона по внедрению цифровых технологий затронули наиболее очевидные общественные отношения: это подача участниками процесса различных заявлений и документов посредством электронного документооборота с применением информационной системы «ГАС Правосудие» и участие в судебном разбирательстве с использованием систем видеоконференцсвязи посредством защищенных каналов связи, урегулированные действующим УПК РФ [2, 13]. Были также предприняты попытки внедрить цифровые технологии в досудебное производство по уголовным делам.

Всеобщее мнение бытует, что с внедрением цифровизации в правосудие, судопроизводство станет более прозрачным. Информация станет доступнее и легче отслеживаться. Внедрение цифровых технологий, таких как автоматизированные системы и электронный документооборот, может значительно уменьшить объем работы и сократить нагрузку на аппарат суда. В некоторых случаях цифровизация позволит проводить заседания с использованием видеоконференцсвязи, что исключит необходимость физического присутствия и, следовательно, уменьшит издержки по непосредственному участию лиц при производстве по уголовному делу.

Вместе с тем, гражданам – участникам процесса, для реализации права подать электронный документ в суд, необходимо иметь электронную подпись (простую, в некоторых случаях – усиленную квалифицированную), полученную через соответствующий онлайн-кабинет, для последующей их идентификации и аутентификации в системе электронного делопроизводства «ГАС Правосудие». Однако, в настоящее время обеспеченность интернет-соединениями распространена не на всей территории страны: в некоторых местах удаленных регионов отсутствует полностью, где-то с ограниченным покрытием, а где-то с ненадлежащим качеством, что является дискуссионным аспектом с точки зрения доступа к правосудию.

Во-вторых, все документы, поступившие в суд посредством электронного документооборота, подлежат переводу на бумажный носитель и соответствующей регистрацией, как документы, поступившие в суд на бумажных носителях. Следовательно, это дополнительная нагрузка на аппарат суда по печати документов и издержки на расходные средства (бумага, работа принтеров и картриджи к ним и др.). Учитывая данный аспект, следует, что в настоящее время судья и аппарат суда формируют производство по уголовным дела как на бумажных носителях, так и в электронном варианте в системе «ГАС Правосудие».

В-третьих, опубликование всех актов, вынесенных в суде, кроме принятых в судебном заседании и зафиксированных в протоколе, с установленными ограничениями подлежат публикации в системе «ГАС Правосудие», и не всегда оно носит автоматический характер, что очевидно, также накладывает дополнительные трудозатраты на аппарат суда.

И, в-четвертых, участие лиц с использованием системы видеоконференцсвязи подразумевает исключения необходимости физического их присутствия. Вместе с тем, это может привести как тактико-криминалистическим и психологическим рискам при проведении следственных и судебных действий (допрос, консультация защитника, ознакомление с материалами дела и др.), так и к проблемам технического характера, связанным как с самой связью осуществляемой по защищенным каналам, так и с технической доступностью соответствующего аппаратного оборудования для проведения сеансов видеоконференцсвязи в достаточном количестве не только в судах, но и в учреждениях правоохранительной системы, в том числе системы исполнения наказаний.

Указанные проблемы и связанные риски, очевидно, не направлены как на ускорение уголовного судопроизводства, так и на минимизацию издержек.

Заключение. Поскольку участники уголовного процесса «молодеют», они, в свою очередь, более мобильны и активно участвуют в интернет-среде, приходя на смену «старому» поколению – «не оцифрованным» людям. Следовательно, подлежат теоретической проработке и более детальному анализу затронутые темы изменений уголовно-процессуального законодательства и те риски, которые неизбежно возникают и могут возникнуть при непосредственной реализации публично-правового регулирования при внедрении цифровых технологий, наметив тем самым пути их разрешения.

Список литературы

1. Баннов А. В. Искусственный интеллект в судебной системе Российской Федерации // Молодой ученый. 2024. № 52 (551). С. 242-246.

2. Бородинова, Т.Г. Цифровые технологии в уголовном судопроизводстве России: пределы и проблемы внедрения. // Правосудие. 2022. №1. С. 71-86. [электронный

ресурс]. URL: https://cyberleninka.ru/article/n/tsifrovye-tehnologii-v-ugolovnom-sudoproizvodstve-rossii-predely-i-problemy-vnedreniya (дата обращения: 01.09.2025).

3. Колоколов, Н.А. Искусственный интеллект в правосудии – будущее неотвратимо. // Вестник Моск. Универ-та МВД России. 2021. № 3. С. 201-211.

4. Концепции развития технологий машиночитаемого права: Протокол Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 15.09.2021 № 31. // СПС «КонсультантПлюс» [электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_396491/ (дата обращения: 19.08.2025).

5. Концепции информатизации Верховного Суда Российской Федерации: Приказ Председателя Верховного Суда РФ от 15.02.2021 № 9-П. // СПС «КонсультантПлюс». [электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_379159/ (дата обращения: 19.08.2025).

6. Маськова, Н.Г., Хажгериева, А.А. Теория поколений: Особенности медиапотребления в условиях активного развития цифровых технологий. // Вестник Майкопского гос. Технолог. Универ-та. 2022. № 4. С. 165-172.

7. Минин, А. Я. Актуальные проблемы цифрового права: учебное пособие для магистрантов и бакалавриата / А. Я. Минин. 2-е изд. Москва: Моск. Педагог. Гос. Универ-ет, 2024. 132 с. ISBN 978-5-4263-0984-5. // Цифровой образовательный ресурс. [сайт]. IPR SMART: [электронный ресурс]. URL: https://www.iprbookshop.ru/146244.html (дата обращения: 19.08.2025).

8. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года: Указ Президента РФ от 07.05.2024 № 309 // СПС «КонсультантПлюс». [электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_475991/ (дата обращения: 19.08.2025).

9. О Центре развития искусственного интеллекта при Правительстве РФ: Постановление Правительства РФ от 09.06.2025 № 861. // СПС «КонсультантПлюс». [электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_507426/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/ (дата обращения: 19.08.2025).

10. Перевозкин, А.А. Теоретико-правовая характеристика машиночитаемого права // Актуальные проблемы российского права. 2024. №8 (165). С. 22-37.

11. Понкин, И.В. Концепт машиночитаемого и машиноисполняемого права. // International Journal of Open Information Technologies. 2020. № 9. С. 57-67. URL: https://cyberleninka.ru/article/n/kontsept-mashinochitaemogo-i-mashinoispolnyaemogo-prava-aktualnost-naznachenie-mesto-v-regtehe-soderzhanie-ontologiya-i-perspektivy (дата обращения: 28.08.2025).

12. Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. Москва: Проспект, 2020. – 640 с. ISBN 978-5-392-22729-7. [электронный ресурс]. URL: https://knigogid.ru/books/1683587-cifrovoe-pravo-uchebnik/toread (дата обращения 13.08.2025)

13. Шереметьев. И. И. Использование цифровых технологий при рассмотрении уголовных дел в суде: реальность и перспективы // Lex Russica. 2019. №5 (150). С. 117-131.

14. Электронное правосудие. Электронный документооборот: научно-практическое пособие. / под общ. ред. С.Ю. Чучи. Москва: Проспект, 2017. 240 с. ISBN 978-5-392-25329-6. [электронный ресурс]. URL: https://thelib.net/2339775-jelektronnoe-pravosudie (дата обращения 20.08.2025)