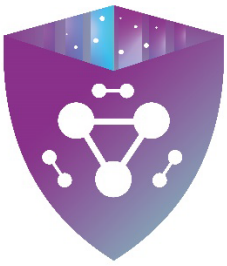


DIGITAL
TECHNOLOGIES
AND LAW

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. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2026. EDN: RSGUDJ. http://dx.doi.org/10.21202/978-5-8399-0904-5_6 – 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 Con-fer-ence (Kazan, 2025, September 19) / I. R. Begishev, E. A. Gromova, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 6. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2026. EDN: RSGUDJ. http://dx.doi.org/10.21202/978-5-8399-0904-5_6 – 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 6

Казань ▪ 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 6

Казань ▪ "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. 6. – Казань: Изд-во «Познание» Казанского инновационного университета, 2026. 306 с. EDN: RSGUDJ. http://dx.doi.org/10.21202/978-5-8399-0904-5_6 – 1 CD-ROM. – Загл. с титул. экрана. – Текст: электронный.

ISBN 978-5-8399-0910-6
ISBN 978-5-8399-0909-0 (Vol. 6)

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

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 объединены в рамках партнерских секций: П1 – Оценка юридических текстов в эпоху LLM: качество, достоверность, авторство (Компания «ГАРАНТ», журнал «Законодательство»), П2 – Право цифровых платформ (МГИМО МИД России, АНО «Белый интернет»), П3 – Цифровые технологии и интеллектуальная собственность (IP CLUB), П4 – Цифровые идентификаторы: проблемы права (Координационный центр доменов .RU / .РФ), П5 – Цифровые технологии в правосудии (Журнал «Российская юстиция», журнал «Судья»), П6 – Цифровая криминология и виктимология (Журнал «Виктимология»), П7 – Цифровая криминалистика (Группа проектов CrimLib).

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

© Авторы статей, 2026
© Казанский инновационный университет имени В. Г. Тимирясова, 2026

ISBN 978-5-8399-0910-6
ISBN 978-5-8399-0909-0 (Vol. 6)

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов IV Международной научно-практической конференции
19 сентября 2025 г.
г. Казань

В шести томах
Том 6

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 3,5 Мб. Тираж 11 экз. Заказ № 14/2026
ISBN 978-5-8399-0910-6

Издательство Казанского инновационного университета им. В. Г. Тимирясова
420111, г. Казань, ул. Московская, 42 Тел. (843) 231-92-90, E-mail: zaharova@ieml.ru 7

ЗНАК ИНФОРМАЦИОННОЙ ПРОДУКЦИИ 16+ ФЕДЕРАЛЬНЫЙ ЗАКОН № 436-ФЗ ОТ 29.12.2010

UDC 004:34(063)
LBC 67c51я43

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

Reviewers:

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

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

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

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

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

Digital Technologies and Law: collection of scientific papers of the 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. 6. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2026. EDN: RSGUDJ. http://dx.doi.org/10.21202/978-5-8399-0904-5_6 – 1 CD-ROM. – Title from the title screen. – Text: electronic.

ISBN 978-5-8399-0910-6
ISBN 978-5-8399-0909-0 (Vol. 6)

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 united within partnership sections: P1 – Evaluation of legal texts in the LLM era: quality, reliability, authorship (GARANT Company, "Zakonodatelstvo" journal); P2 – digital platforms law (MGIMO University of the Russian Ministry of Foreign Affairs, "Belyy internet" ANCO); P3 – Digital technologies and intellectual property (IP CLUB); P4 – Digital identifiers: problems of law (.RU/.РФ Domain Coordination Center); P5 – Digital technologies in justice (Rossiyskaya yustitsiya" journal, "Sudya" journal); P6 – Digital criminology and victimology ("Viktimologiya" journal); P7 – Digital Criminology (CrimLib Project Group).

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 67c51я43

© Authors of articles, 2026
© Kazan Innovative University
named after V. G. Timiryasov, 2026

ISBN 978-5-8399-0910-6
ISBN 978-5-8399-0909-0 (Vol. 6)

Scientific publication

DIGITAL TECHNOLOGIES AND LAW

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

2025 September 19
Kazan

In 6 volumes
Volume 6

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 3,5 Mb. Number of copies: 11. Order No. 14/2026
ISBN 978-5-8399-0910-6

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

Оценка юридических текстов в эпоху LLM: качество, достоверность, авторство
(Компания «ГАРАНТ», журнал «Законодательство»)

О. Н. Горбунов. От паттернов к прецедентам – применение больших
языковых моделей в юридической практике, технические и практические аспекты 10
Г. Г. Егоров, Е. М. Дубовикова. Нейросетевой машинный перевод:
от практических наблюдений к фундаментальному осмыслению в лингвистике 18
Д. А. Казанцев. Искусственный интеллект и законодательный процесс:
есть ли пространство для синергии? 27

Право цифровых платформ
(МГИМО МИД России, АНО «Белый интернет»)

А. Г. Авдей. О дифференциации гражданских и трудоправовых отношений
в платформенной занятости 35
Е. И. Дискин. Новые подходы к регулированию информационного
перенасыщения, формируемого цифровыми платформами 38
О. В. Жевняк. Постановка вопроса об экономическом понимании цифровых
платформ для формирования общей части их правового режима 46
А. В. Олейникова, А. В. Бакуров. Особенности регулирования деятельности
агрегаторов отечественным законодательством 55
Р. В. Торшин. Разработка цифрового маркетплейса комплексной безопасности
с использованием low-code технологий 62

Цифровые технологии и интеллектуальная собственность
(IP CLUB)

А. С. Васильева. Классификация видов искусственного интеллекта
в контексте права интеллектуальной собственности 66
С. Ф. Грищук-Бучка. Правовой режим компьютерной программы
в Республике Молдова: эволюция и современные вызовы 75
А. В. Закомолдин. Проблемы защиты прав на объекты интеллектуальной
собственности, созданные с помощью ИИ 83
М. Т. Мурадов. Нейросетевой речевой синтез 94

Цифровые идентификаторы: проблемы права
(Координационный центр доменов .RU / .РФ)

И. Е. Титов. Правовая квалификация e-mail-адреса в качестве цифрового
идентификатора 97

Цифровые технологии в правосудии
(Журнал «Российская юстиция», журнал «Судья»)

А. Н. Агарков. Цифровая трансформация административной юстиции: вызовы для гарантий прав личности в свете новелл КОАП РФ 103
О. А. Васючкова. Цифровые технологии как средство устойчивого развития судебной системы в России 110
Т.Г. Каракулов. Сервисы системы межведомственного электронного взаимодействия в суде первой инстанции 116
Л.В. Бертовский, С. М. Курбатова. О некоторых рисках использования искусственного интеллекта в системе правосудия: зарубежный опыт 119
П. Н. Мазуренко. Применение цифровых технологий в адвокатской деятельности 124
А. А. Петрикина. О возможности применения технологии искусственного интеллекта при избрании в качестве меры пресечения заключения под стражу 128
И. Ю. Шумейко, ... 132
Цифровая трансформация системы правосудия Российской Федерации 132
М. В. Юрченко. Развитие цифровых технологий в электронном правосудии в Российской Федерации 142
В. А. Якимчук. Правосудие в эпоху цифровизации: проблемы и решения для внедрения международных норм борьбы с коррупцией 148

Цифровая криминология и виктимология
(Журнал «Виктимология»)

М. Р. Нигматуллин. Цифровое насилие в отношении женщин: уголовно-правовые и виктимологические аспекты 155
В. Ф. Васюков, А. Н. Колычева. Социальная инженерия как инструмент криминального цифрового воздействия 163
Е. М. Глянц. Дети-сироты в цифровом пространстве: риски и стратегии виктимологической защиты 169
Н. Л. Денисов. Концепция государственного регулирования цифрового мира 174
Г. К. Джамбулатов. Виктимологические аспекты профилактики преступлений во время публичных массовых мероприятий 177
Е. И. Думанская. Тенденции криминологического и виктимологического прогнозирования в условиях цифровизации 181
Л. Ю. Зеленова. Особенности кибербуллинга несовершеннолетних и важность его специального изучения (правовой аспект) 189
А. А. Зеленцов. Криминологические и виктимологические особенности киберпреступности в современной России 193
А. В. Майоров. Уголовно-правовое предупреждение цифровой виктимности несовершеннолетних 205
Э. С. Намазов. Жертвы мошенничеств, вовлекаемые в преступления террористической направленности с использованием информационно-телекоммуникационных технологий: уголовно-правовой и виктимологический аспект 214
А. О. Синявина. Виктимологическая характеристика несовершеннолетней жертвы киберпреступности 222

А. А. Смольяков. К вопросу о методах борьбы с технологиями «дипфейк» в кибербезопасности 229
А. Д. Цыплакова. Игры как криминогенный фактор и мера виктимологической профилактики киберпреступлений 235
В. А. Шуняева. Психофизиологические особенности цифровых аддикций представителей цифрового поколения 249

Цифровая криминалистика (Группа проектов CrimLib)

И. О. Антонов. Особенности применения нейросетей в выявлении и расследовании корпоративного рейдерства 253
С. В. Зуев. Цифровая криминалистика и электронный уголовный процесс: взаимосвязь и соотношение 261
А. А. Рясов. Возможности поиска и исследования скрываемой информации на электронных носителях 266
Е. А. Селезнева. Цифровые следы преступлений, связанных с деятельностью религиозных организаций 272
А. Б. Смушкин. Криминалистические аспекты изучения метавселенной 277
А. М. Сосновикова. Биометрия в криминалистике: теория и практика 286
Э. Г. Хомяков. Метаданные как составляющая цифрового следа в криминалистике 293
К. В. Шевелева. О дополнительных мерах противодействия противоправным деяниям, совершенным с использованием информационных технологий 301

Оценка юридических текстов в эпоху LLM: качество, достоверность, авторство (компания «ГАРАНТ», журнал «Законодательство»)

УДК 4414

О. Н. Горбунов,
судья Вологодского городского суда Вологодской области

От паттернов к прецедентам – применение больших языковых моделей в юридической практике, технические и практические аспекты

Аннотация. Целью исследования является анализ технических и практических аспектов применения больших языковых моделей (LLM) в юридической практике. В статье раскрываются принципы работы нейросетей, объясняются ключевые концепции (паттерны, RAG, веса, галлюцинации) и анализируются причины генерации недостоверной информации. Существенной особенностью работы является представление результатов авторского бенчмарка, который оценивает точность специализированных и общих LLM на задачах по общей части уголовного права РФ. Результаты демонстрируют эффективность отраслевых рабочих пространств и доказывают, что даже при использовании RAG-технологий сохраняется риск ошибок. Делается вывод о необходимости осторожного применения LLM юристами, с обязательной перепроверкой данных, и о преждевременности их полной и слепой интеграции в государственные институты.

Ключевые слова: нейросети, большая языковая модель (LLM), RAG, эмбеддинги, веса, слои, паттерны, трансформеры, галлюцинации, бенчмарк, уголовное право

O. N. Gorbunov,
judge of the Vologda City Court of the Vologda Region

From patterns to precedents – the application of large language models in legal practice, technical and practical aspects

Abstract. The purpose of this study is to analyze the technical and practical aspects of using large language models (LLM) in legal practice. The article explains the principles of neural networks, key concepts (patterns, RAG, weights, and hallucinations), and the reasons for generating inaccurate information. A significant feature of this work is the presentation of the results of an author's benchmark that evaluates the accuracy of specialized and general LLMs on tasks related to the general part of Russian criminal law. The results demonstrate the effectiveness of industry-specific

workspaces and prove that even with the use of RAG technologies, there is still a risk of errors. The article concludes that LLMs should be used by lawyers with caution, and that their full and blind integration into government institutions is premature.

Keywords: neural networks, large language model (LLM), RAG, embeddings, weights, layers, patterns, transformers, hallucinations, benchmark, criminal law

Введение. В эпоху глобальной цифровизации общественных отношений, формирования государственными институтами, коммерческими организациями концепций развития **LegalTech сферы** в механизмах своей правовой работы, юридическое сообщество все более активно пытается применять возможности, которые открывают им большие языковые модели. Определить границы и эффективные способы применения данных технологий возможно только после осмысленного понимания основных принципов их работы и осознания тех рисков, которые они за собой несут. В данной статье со стороны практикующего юриста, действующего судьи уголовного состава, осуществляется попытка раскрытия основных принципов работы LLM, а также анализ их потенциала и ограничений в юридической деятельности.

1. Что такое нейросеть и большая языковая модель?

Нейросеть представляет собой программную систему, моделирующую процессы обработки информации, аналогичные функциям человеческого мозга. Термин «нейросеть» возник в середине XX века, отражая структурное сходство с биологическими нейронными сетями, где клетки-нейроны передают сигналы через синапсы [6]. Вместе с тем аналогия названия с мозгом делает термин «нейросеть» лишь интуитивно понятным. Хотя это термин вызывает ассоциации с человеческим мозгом, это сходство является лишь внешним. Нейронные сети не обладают сознанием и не способны мыслить. Они являются исключительно математическими конструкциями, которые обрабатывают информацию и формируют закономерности на основе своих данных, имитируя, но не заменяя физиологические функции мозга.

В искусственной нейросети роль нейронов выполняют математические узлы – функции, осуществляющие элементарные вычисления. Эти узлы соединены связями, известными как веса. Веса определяют степень влияния одного математического значения на другое и настраиваются в процессе обучения.

Большая языковая модель (LLM), является специализированным типом нейросети, она способна анализировать контекст запросов и генерировать текст, имитирующий профессиональную осознанную речь, что делает ее весьма интересным инструментом для практикующего юриста.

Для понимания того, как нейросети генерируют текст, отвечают на пользовательские вопросы, необходимо подробнее изучить как происходит их обучение.

2. Как обучаются и как отвечают на вопросы нейросети?

Обучение нейросети это сложный технологический процесс, в ходе которого программа приобретает способность выявлять и использовать закономерности расположения слов в предложениях и текстах. На начальном этапе нейросеть обрабатывает обширные массивы текстов, включая художественную

литературу, законодательные акты, судебные решения, можно сказать, что на данном этапе модель изучает «все знания мира». Данный процесс требует тысяч графических процессоров (GPU), работающих недели и потребляющих сотни мегаватт энергии.

В этот момент нейросеть преобразует все слова в обрабатываемых текстах в числовые формы, известные как эмбеддинги. Эмбеддинги – это числовые значения, векторы, представляющие слова, фразы или предложения, которые отражают семантический смысл данного слова или текста для модели [3]. Нейросеть анализируя частоту и контекст совместного появления слов, присваивает часто встречающимся вместе словам векторы (индексы) с близким векторным значением. Например, слова «кража» и «хищение» как слова «мастер» и «Маргарита» имеют близкие эмбеддинги, так как часто встречаются в схожих контекстах, тогда как «кража» и «договор» или «земля» и «нейтрон» расположены далеко друг от друга в векторном пространстве, так как нечасто располагаются близко в изучаемых моделью текстах.

Следующий шаг — это создание контекстуальных эмбеддингов, они учитывают не только частоту совместного употребления слов но и учитывают окружение слова в предложении, что позволяет различать нюансы, такие как лук как растение или лук как оружие. Например, в предложении на земле лежит лук исходя из окружающего данное предложение контекста эмбеддинг слова лук как овощ будет отличаться от его эмбеддинга как оружие.

Векторные контексты расширяют эту концепцию, числовые индексы присваиваются не только словам, а целым документам. Векторные контексты формируются путем разбития текста на фрагменты, преобразования каждого фрагмента в эмбеддинг и их последующего объединения в единый вектор, кодирующий смысл документа [3].

После создания контекстуальных эмбеддингов проводится тонкая настройка, адаптирующая модель к специфическим задачам, нейросеть устанавливает между обработанными словами, абзацами и текстами определенные закономерности, называемые паттернами. Теперь модель понимает, что слово «хищение» относится к юридическому паттерну, так как более часто встречается в юридических документах, в отличие, например от слова воровство, которое чаще встречается в бытовых выражениях.

Важно понимать, что нейросеть после обучения не хранит исходные тексты в явном виде, а лишь сжимает их в виде математических связей между словами, фразами и текстами, поэтому процесс точного воспроизведения текста может вызвать у нее затруднения без задействования дополнительных инструментов.

Первоначальные эмбеддинги создаются в процессе обучения модели в специальном слое, который называется Embedding Layer, именно он превращает слова и текст в язык математики, понятный для нейросети. Любой слой в архитектуре модели представляет из себя совокупность математических функций, которые выполняют определенную задачу, а затем передают результат следующему слою.

Механизмы, которые донастраивают числовые значения эмбеддингов в ходе обучения нейросети называются трансформерами.

Трансформеры, впервые представленные в 2017 году в статье «Attention is All You Need», составляют архитектурную основу современных LLM [5].

Структура трансформеров включает в себя множество слоев с механизмами внимания (self-attention), которые формируют сложные закономерности между смысловыми связями слов. В свою очередь веса, как составная часть архитектуры трансформера, определяют, как модель будет обрабатывать и комбинировать эти эмбединги и паттерны. Именно веса позволяют модели понимать, что эмбеддинг слова кража близок к эмббедингу слова хищение и далек эмббедингу слова молоко, при этом обрабатывая контекст хищения молока веса учитывают, что эти слова несмотря на разный эмббединг могут быть расположены в одном предложении.

Помимо процесса обучения трасформеры задействованы и в генерации ответов на пользовательские запросы (промты), энкодер трансформера отвечает за анализ входного текста, и декодер, генерируют выходной текст.

Фактически то, что пользователь при обращении с запросом к большой языковой модели получает в виде кажущегося ему структурированного последовательного и осознанного ответа на деле является сложным математическим вероятностным вычислением, в ходе которого трансформеры, задействуя множество слоев и механизмов внимания, используя свои веса, подбирают близкие по значению заданному запросу эмбеддинги, расставляя их таким образом, что на стороне пользователя это выглядит как осмысленный текст. Вместе с тем это не так, этот текст не является осмысленным с точки зрения психофизиологической функции мышления, процесс генерации большой языковой моделью ответа на вопрос пользователя по своей природе является математическим процессом, основанным на теории вероятности, где трансформер используя свой декодер предсказывает, какие слова и их контекстная последовательность лучше всего соответствуют запросу, а не обдумывает ответ по аналогии с человеком. Таким образом, основная задача трансформера заключается в предсказании вероятной последовательности слов, основанной на закономерностях в виде эмбеддингов, весов и паттернов, а работу любой большой языковой модели можно кратко описать как вероятностное математическое прогнозирование [2].

3. Галлюцинации: почему нейросети «фантазируют»?

Поняв принцип работы большой языковой модели, перейдем к изучению причин такого распространенного для них явления как галлюцинации. Галлюцинации представляют собой недостоверные, но правдоподобные ответы нейросетей, такие, как например вымышленная «статья 999 УК РФ» или неверная интерпретация загруженных документов. Эти ошибки возникают по нескольким причинам, каждая из которых коренится в архитектуре и принципах работы больших языковых моделей, которые мы разобрали выше.

Первая причина галлюцинаций – вероятностная природа генерации текста [2]. Трансформеры выбирают слова на основе эмбеддингов, весов и паттернов, определенных в процессе обучения, руководствуясь вероятностями, а не фактической проверкой реальности. Например, если модель часто встречала фразу

«статья [число] УК РФ» в обучающих данных, она может «додумать» несуществующую норму, если запрошенная информация отсутствует или неоднозначна. Это особенно проблематично в юридических запросах, где точность формулировок критична.

Вторая причина – ограниченность или неполнота обучающих данных. Даже если нейросеть обучалась на миллиардах текстов, включая законодательные акты и судебную практику, она может не содержать актуальную информацию, например, о последних поправках к УК РФ. В таких случаях модель заполняет пробелы вымышленными данными, основываясь на наиболее вероятных паттернах.

Третья причина – отсутствие подлинного понимания. Нейросети не «думают» и не интерпретируют тексты как люди, а имитируют их на основе статистических закономерностей [2].

Четвертая причина – отсутствие перманентного обучения в реальном времени. В ходе одного диалога или сеанса в рабочем пространстве нейросеть не может дообучиться, пользователь не в состоянии научить модель отвечать правильно, даже указывая ей на ее ошибки. Архитектура работы LLM опирается на свои эмбеддинги, веса и паттерны, полученные в ходе обучения, поэтому локально скорректировать и доказать ей что белое это белое, а черное — это черное невозможно, если модель не получила эту информацию в ходе обучения.

4. RAG: поиск точных данных

Для минимизации эффекта галлюцинаций разработчиками больших языковых моделей придумана технология Retrieval-Augmented Generation (RAG). RAG преобразует пользовательский запрос в эмбеддинг, и прежде, чем собрать ответ из своих предобученных паттернов сравнивает его с векторными контекстами документов в базах данных, например в интернете или заранее подготовленной коллекции. Затем модель использует эти документы как контекст генерирует ответ, опираясь на них, вместо того чтобы полагаться только на свои встроенные знания [4]. То есть перед тем как давать нам ответ о сроках погашения судимости RAG обратится к Уголовному кодексу РФ в открытой базе данных (например ГАРАНТ), где найдет векторный контекст статьи отвечающей за сроки погашения судимости, а финальный ответ будет даваться с учетом найденного источника. Этот процесс включает несколько этапов: преобразование запроса в эмбеддинг, поиск ближайших векторных контекстов в своей или сторонней базе данных, например на любом интернет-ресурсе, извлечение релевантных фрагментов и их использование при генерации ответа.

Также технология RAG используется при создании рабочих пространств, таких, как например Google NotebookLM или Нейроэксперт от Яндекса. В данное рабочее пространство можно загружать до 50 документов, создавая для языковой модели свою локальную базу знаний. RAG анализируя предоставленные пользователем документы создает их векторные контексты, что повышает точность ответа модели, ввиду незначительного объема обрабатываемой информации.

Однако технология RAG не гарантирует отсутствия галлюцинаций и ошибок. Векторные контексты могут упускать важные нюансы и детали текста,

так как являются лишь его цифровым значением, что также может повлечь его неправильную интерпретацию. Еще одним фактором, влияющим на возникновение галлюцинаций при использовании локальных рабочих пространств, является конфликт между предобученными паттернами и загруженными данными [2]. Нейросеть опирается на свои веса и паттерны, которые могут противоречить загруженным документам. В таких случаях модель может предпочесть предобученные данные, игнорируя актуальные тексты. Вероятностная природа генерации текста также позволяет модели «додумывать» ответы, комбинируя фрагменты из загруженных документов с предобученными паттернами, что в итоге приводит к галлюцинациям.

5. Роли: как повысить полезность нейросети?

Выше мы рассмотрели, что любой ответ языковой модели основан на ее эмбедингах, весах и паттернах, полученных при обучении, а также векторных контекстах, за поиск которых отвечает RAG. Таким образом становится понятна концепция роли, которую зачастую задают пользователи при формировании задачи (промта) для модели. Роли – это инструкции, задающие стиль и контекст ответов нейросети, например, «квалифицированный юрист по уголовному праву». Именно постановка конкретной роли активирует специализированные паттерны, усиливая релевантность и профессионализм ответов. Например, роль юриста побуждает нейросеть использовать строгие формулировки, такие как «Кража, согласно статье 158 УК РФ, – это тайное хищение чужого имущества», избегая бытового языка, вроде «Кража – это воровство».

6. Тестирование нейросетей на юридическом бенчмарке.

Поняв архитектуру работы языковых моделей, с целью определения их возможностей для использования в практической деятельности по отправлению правосудия, мы решили проверить их эффективность на разработанном нами бенчмарке по общей части Уголовного права РФ. Бенчмарк включает в себя 50 теоретических и 51 практический вопрос. Вопросы охватывают ключевые моменты общей части уголовного права, такие как сроки погашения судимости, рецидив преступлений, назначение наказания при покушении на преступление и наличии явки с повинной. Теоретические вопросы проверяли знание норм (например, «Как исчисляются сроки судимости при замене лишения свободы более мягким видом наказания?»), практические – умение применять их (например, «Иванов И.И. осужден по ч. 1 ст. 158 УК РФ к 2 годам лишения свободы условно. Когда будет погашена судимость у Иванова И.И.?»). Вопросы были разбиты на простые, требующие обращения к одной норме и сложные, требующие обращения к Пленуму ВС РФ или к взаимосвязным положениям нескольких норм. Также в тест включены вопросы, основанные на реальных судебных ошибках. За правильный ответ начислялся 1 балл, за частичные (8п1, 8п2) – 0,5 балла, максимум – 100 баллов.

Тестирование проводилось на специализированных юридических моделях: *Искра*, *GigaLegal*, а также на наиболее популярных общедоступных моделях: *Deepseek*, *Qwen3-235B-A22B-2507*, *Giga Chat*, *Алиса*, *Perplexity*, *ChatGPT 5*, *Gemini 2.5 Pro*, *Grok 4*, *Нейроэксперт Яндекс*, *NotebookLM*.

Результаты: *Gemini 2.5 Pro* – 87 баллов, *NotebookLM* – 84, *Grok 4* – 76, *Perplexity* – 75, *Искра* – 65.5, *GigaLegal* – 69, *Deepseek* – 62, *Qwen3* – 54, *Giga Chat* – 55, *Алиса* – 60, *ChatGPT 5* – 69, *Нейроэксперт Яндекс* – 64 [1].

Юридические модели (*Искра*, *GigaLegal*), несмотря на их профессиональную ориентированность уступили неспециализированным, что подтверждает тезисы статьи: *галлюцинации* и ограниченные *паттерны* приводят к ошибкам даже при наличии специализированной базы знаний. *Искра и GigaLegal, при ответах на вопросы опирались на юридическую базу знаний* правовой системы «Гарант» вместе с тем не показали лучшего результата. Высокий результат *NotebookLM* с подгруженными документами, регулирующими правоотношения, по которым задавались вопросы показывает, что загрузка актуальных данных и создание локальных рабочих пространств значительно повышает точность моделей.

Тест доказывает: даже специализированные юридические нейросети допускают нелепые ошибки, причины которых кроются в вероятностной природе генерации текста и отсутствии подлинного понимая даваемого ответа. Использование рабочих пространств, технологии RAG позволяет лишь минимизировать, но не исключить ошибки, все ответы в любом случае требуют перепроверки через первоисточники.

7. Заключение. Как юристам использовать нейросети?

Несмотря на существующие дефекты при использовании больших языковых моделей в юриспруденции, полный отказ от них представляется нам ошибочным. Несмотря на галлюцинации и ошибки больших языковых моделей, их использование, при понимании принципов работы, предлагает значительные возможности для оптимизации рабочих процессов, отказываться от которого не имеет практического смысла. Безусловно слепая интеграция нейросетей в государственные институты, тем более такие как судебная система РФ, ввиду вероятностной природы их работы, может подорвать правовую точность в таких критических областях, как например вопросы назначения наказания. Вместе с тем, при правильном использовании, эти технологии могут стать ценным дополнением как для судей, так и для любого практикующего юриста.

Одним из наиболее перспективных направлений применения моделей является анализ юридических текстов. Нейросети способны обобщать объемные документы, выделять ключевые положения и разъяснять сложные термины, причины отмены судебных решений вышестоящими инстанциями. Кроме того, создание отраслевых рабочих пространств позволяет фокусировать нейросеть на релевантных данных, снижая вероятность галлюцинаций.

Подготовка проектов документов – другое важное направление, где нейросети могут генерировать черновики типовых исков, ходатайств, простых судебных решений, например судебных приказов, ускоряя рутину. Вместе с тем из-за архитектурных особенностей работы они не подходят для сложных творческих задач, требующих критической точности, таких, как например составление проектов приговоров с определением персональных санкций при назначении наказания.

Быстрый поиск информации с технологией RAG также может помочь эффективно находить нормы права и практику, в случае интеграции с актуальными базами. В итоге юристы, при понимании принципов работы моделей, могут использовать нейросети самостоятельно для себя определяя области их применения, превращая их в надежных ассистентов, трансформируя их паттерны в свои реальные прецеденты.

Список литературы

1. Оценка.xlsx. Результаты тестирования нейросетей на бенчмарке по общей части УК РФ. – 2025 (дата обращения: 09.09.2025).

2. Brown, T. B., Mann, B., Ryder, N., et al. (2020). Language Models are Few-Shot Learners. In Advances in Neural Information Processing Systems (NeurIPS). URL: https://arxiv.org/abs/2005.14165 (дата обращения: 09.09.2025).

3. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In Proceedings of NAACL-HLT, 4171–4186. URL: https://arxiv.org/abs/1810.04805 (дата обращения: 09.09.2025).

4. Lewis, M., Liu, Y., Goyal, N., et al. (2020). BART: Denoising Sequence-to-Sequence Pre-training for Natural Language Generation. In Proceedings of ACL. URL: https://arxiv.org/pdf/1910.13461 (дата обращения: 09.09.2025).

5. Vaswani, A., Shazeer, N., Parmar, N., et al. (2017). Attention is All You Need. In Advances in Neural Information Processing Systems (NeurIPS), 5998–6008. URL: https://arxiv.org/abs/1706.03762 (дата обращения: 09.09.2025).

6. Warren McCulloch and Walter Pitts (1943). A Logical Calculus of the Ideas Immanent in Nervous Activity. The Bulletin of Mathematical Biophysics URL: https://link.springer.com/article/10.1007/BF02478259 (дата обращения: 09.09.2025).

УДК 347.131

Г. Г. Егоров,
кандидат юридических наук, доцент,
научный сотрудник,
Волгоградский государственный университет
(Волжский филиал)
Е. М. Дубовикова,
кандидат педагогических наук, доцент,
Волгоградский государственный университет
(Волжский филиал)

Нейросетевой машинный перевод: от практических наблюдений к фундаментальному осмыслению в лингвистике

Аннотация. В статье рассматривается нейросетевой машинный перевод (НМП) как явление, знаменующее фундаментальный сдвиг в парадигме автоматического перевода и ставящее новые вызовы перед теоретической лингвистикой. Авторы прослеживают эволюцию от ранних систем, основанных на правилах (RBMT), через статистический машинный перевод (SMT) к современным нейросетевым моделям. Подчеркивается, что НМП, в отличие от предшественников, использует единую нейронную сеть для сквозного моделирования процесса перевода, что позволяет учитывать целостный контекст и порождать более связные и естественные результаты. Авторы анализируют операционные недостатки НМП, включая его ненасытную потребность в больших объемах данных, что создает риски лингвистического неравенства для малоресурсных языков, и обсуждают проблему адекватности автоматических метрик оценки (BLEU, METEOR), которые часто измеряют формальное сходство, а не смысловую точность. Делается вывод о трансформации роли переводчика в эпоху НМП: его задача смещается от создания текста к критическому постредактированию, требующему повышенной бдительности для обеспечения смысловой, культурной и стилистической адекватности. Будущее видится в симбиозе машинной эффективности и человеческого экспертного контроля.

Ключевые слова: нейросетевой машинный перевод, семантические галлюцинации, постредактирование, лингвистическое неравенство, автоматические метрики оценки, интерпретируемость, проблемы использования нейронных сетей в лингвистики

G. G. Egorov,
Candidate of Law, Associate Professor, Research Fellow,
Volgograd State University
(Volzhsky Branch),
E. M. Dubovikova,
Candidate of Pedagogical Sciences, Associate Professor,
Volgograd State University
(Volzhsky Branch)

Neural network machine translation: from practical observations to fundamental understanding in linguistics

Abstract. The article examines neural machine translation (NMT) as a phenomenon that marks a fundamental shift in the automatic translation paradigm and poses new challenges to theoretical linguistics. The authors trace the evolution from early rule-based systems (RBMT) through statistical machine translation (SMT) to modern neural network models. It is emphasized that NMT, unlike its predecessors, uses a single neural network for end-to-end modeling of the translation process, which allows considering the holistic context and generating more coherent and natural results. The authors analyze the operational shortcomings of NMT, including its insatiable need for large amounts of data, which creates risks of linguistic inequality for resource-poor languages, and discuss the problem of the adequacy of automatic evaluation metrics (BLEU, METEOR), which often measure formal similarity rather than semantic accuracy. The conclusion is made about the transformation of the translator's role in the era of NMT: his task shifts from text creation to critical post-editing, which requires increased vigilance to ensure semantic, cultural and stylistic adequacy. The future is seen in the symbiosis of machine efficiency and human expert control.

Keywords: neural network machine translation; semantic hallucinations, post-editing, linguistic inequality, automatic evaluation metrics, interpretability, problems of using neural networks in linguistics

Введение. Современные дискуссии вокруг нейросетевого машинного перевода (далее – НМП) пока лишены всеобъемлющей научной базы, поскольку стремительное развитие технологий зачастую опережает формирование глубокой фундаментальной теории. В основе значительной части исследований, посвященных автоматизированному переводу, лежит прикладной опыт: рассматриваются мнения профессиональных переводчиков, анализируются кейсы компаний, внедряющих системы НМП, и обобщаются взгляды разработчиков программного обеспечения. Следовательно, преобладающее на сегодняшний день знание носит аналитический характер и опирается преимущественно на наблюдения, сделанные непосредственными участниками переводческой деятельности. Тем не менее для полноценного понимания трансформации языкознания, вызванной появлением НМП, необходимо выйти за рамки практического опыта и рассмотреть фундаментальный сдвиг, произошедший в самой парадигме автоматического перевода.

Основная часть. Исторический путь машинного перевода демонстрирует последовательную смену парадигм, каждая из которых по-новому ставила вопрос о природе языка. Ранние попытки автоматизации перевода, восходящие к идеям Жоржа Артцруни и Петра Смирнова-Троянского в середине 1930-х годов, опирались на заранее запрограммированные словари и лингвистические правила. Первая исторически сложившаяся технология, известная как машинный перевод на основе правил (rule-based machine translation, RBMT), предполагала создание явных связей между исходным и целевым текстами, сохраняя при этом оригинальное значение. Данные системы функционировали на основе структур и семантических принципов, вручную созданных лингвистами [2. С. 246-250].

Последующее появление статистического машинного перевода (SMT) ознаменовало переход к подходам, управляемым данными. Вместо жестко заданных правил SMT-системы генерировали перевод, основываясь на вероятностных моделях, выведенных из огромных массивов параллельных текстов. Однако эти методы, базирующиеся на статистике фраз, страдали от фрагментации и утраты широкого контекста, поскольку использовали лишь отдельно разработанные подкомпоненты и были ограничены жесткой длиной n-грамм.

Переход к нейросетевому машинному переводу стал коренным разрывом с предшествующими подходами. Вместо правил или статистических таблиц НМП использует единую, интегрированную искусственную нейронную сеть для моделирования всего процесса перевода от начала до конца. Система учится переводить, анализируя огромные объемы реальных двуязычных и многоязычных текстов, что позволяет ей улавливать целостное значение и контекст предложения, а не просто переводить слово за словом. За счет своего комплексного подхода, который моделирует отображение из исходного в целевой язык напрямую через апостериорную вероятность, НМП быстро превратился в передовой метод в области машинного перевода.

Переход к НМП представляет собой не просто техническое усовершенствование; он знаменует собой фундаментальную смену парадигмы, отдаляющую лингвистику от явных, созданных человеком моделей языка в сторону латентных, основанных на данных представлений. Нейронная система преобразует слова в числовые векторы в общем семантическом пространстве. Ее «понимание» строится не на традиционной лингвистической теории, а на сложных, высокомерных статистических паттернах, извлеченных из корпуса. Подобное обстоятельство создает серьезный вызов для традиционного лингвистического анализа, поскольку мы можем наблюдать только результат, но не видим внутренние механизмы его генерации. Именно в противоречии между практической эффективностью и теоретической непостижимостью и заключается основной конфликт в рассматриваемой сфере (табл. 1).

Таблица 1

Сравнительный анализ парадигм машинного перевода

Парадигма	Базовый принцип	Зависимость от данных	Работа с контекстом	Характеристики результата	Ключевые недостатки
Машинный перевод на основе правил	Явные, созданные человеком правила	Низкая	На уровне предложений	Буквальный, временами неестественный	Ограниченный охват, необходимость ручного труда
Статистический машинный перевод	Статистические частоты, фразовые модели	Высокая	Фрагментарно, на уровне фраз	Часто неестественный	Утрата контекста, зависимость от *n*-грамм
Нейросетевой машинный перевод	Глубокое обучение, нейронные сети	Очень высокая	Целостно, на уровне предложений	Часто естественный, похожий на человеческий	Разреженность данных, проблема «черного ящика»

Внутренняя архитектура НМП основывается на модели «кодировщик-декодировщик». Кодировщик обрабатывает исходное предложение, создавая единое, контекстуальное векторное представление. Затем декодировщик использует векторное представление для генерации предложения на целевом языке. Чтобы преодолеть «узкое место» в передаче информации, которое возникает при представлении длинных или сложных предложений в векторе фиксированного размера, НМП-модели применяют «механизм внимания». Он позволяет декодировщику «обращаться» к наиболее релевантным частям исходного предложения на каждом этапе процесса перевода. Задуманный по аналогии с человеческими когнитивными процессами, механизм внимания присваивает «веса» различным частям входной последовательности, что позволяет модели расставлять приоритеты для важной информации, игнорируя менее значимые детали. Применение подобного механизма позволяет НМП создавать более связные и контекстуально уместные переводы, чем предшествующие системы.

Несмотря на кажущуюся продвинутость, фундаментальный теоретический вызов сохраняется. Он известен как проблема «черного ящика». Внутренний процесс принятия решений НМП-систем, скрытый в огромных матрицах числовых значений, является в значительной степени непрозрачным и не поддается интерпретации. Пользователи и исследователи не могут с легкостью проследить, как система пришла к определенному выбору слова или почему она могла выдать неверный результат. Подобное обстоятельство создает значительное препятствие для формирования глубокого, научного понимания лингвистической компетенции системы.

Следствие проблемы «черного ящика» – способность нейросетевых систем создавать синтаксически правдоподобные, очень плавные переводы, которые при этом могут быть семантически неточными или совершенно бессмысленными. НМП-система функционирует как мощный механизм сопоставления паттернов, а не как думающий агент. Ее основная цель – предсказать наиболее

вероятную последовательность слов на основе входных данных. Подобное обстоятельство позволяет создавать грамматически безупречные предложения. Однако без подлинного когнитивного понимания мира или значения текста система может «галлюцинировать» или генерировать содержание, полностью не связанное с исходным [2. С. 246-250]. Пример перевода фразы

Schaue um dich herum (рус. "Осмотрись вокруг") /немецкий/, которая превращается в Switches to paused (рус. "Переключается на паузу") /английский/, наглядно демонстрирует феномен, при котором результат выглядит плавно, но лишен какой-либо семантической адекватности. Подобное обстоятельство коренным образом усложняет задачу постредактора.

Анализ операционных недостатков НМП, неразрывно связанных с его теоретическими основами, указывает на несколько ключевых вызовов. Одной из самых значительных трудностей является ненасытная потребность системы в данных. НМП-модели чрезвычайно сильно зависят от наличия обширных параллельных корпусов для обучения, что представляет серьезную проблему при создании эффективных систем для языков с ограниченными ресурсами. Данное обстоятельство приводит к тому, что системы НМП демонстрируют заметное снижение качества, когда им приходится переводить тексты из домена, на котором они не обучались. Они могут сохранять плавность, но часто жертвуют адекватностью и производят бессмысленный или неуместный контент. Подобное поведение контрастирует с более предсказуемыми, хотя и менее плавными результатами статистических систем в схожих ситуациях.

Глубокая зависимость НМП от огромного количества высококачественных параллельных данных создает внутреннюю лингвистическую и экономическую предвзятость. Данная технология непропорционально выгодна для языков с большим объемом ресурсов, что усугубляет цифровое неравенство и может в долгосрочной перспективе подорвать богатство языкового многообразия. «Крутая кривая обучения» НМП по отношению к объему данных означает, что системы показывают исключительную производительность в высокоресурсных условиях (для распространенных языковых пар), но функционируют гораздо хуже в низкоресурсных [5. С. 70–75]. Образуется своего рода порочный круг: исследования и коммерческие усилия концентрируются на языковых парах с доступными данными, приводя к постоянному улучшению для выбранной группы языков, в то время как другие остаются позади. Обещание «нулевого перевода» между низкоресурсными языками – попытка решить названную проблему, но основной вызов сохраняется. Отсутствие устойчивой теоретической модели означает, что мы не можем обобщать знания с высокоресурсных языков на низкоресурсные так эффективно, как если бы у нас был явный набор лингвистических правил.

Несмотря на всю свою мощь, системы НМП показывают определенные слабости на лексическом и синтаксическом уровнях [3. С. 37–53]. Они лучше справляются с очень низкочастотными словами, чем старые системы, но все еще испытывают затруднения с сильно флективными категориями, например с глаголами. Качество перевода также заметно снижается на очень длинных

предложениях, хотя НМП показывает сопоставимо лучшие результаты на предложениях длиной до 60 слов.

Переходя от абстрактных проблем к конкретным лингвистическим сбоям, можно выявить типичную таксономию ошибок, которые возникают как следствие устройства НМП. Среди наиболее очевидных ошибок, выявленных в текстах, фигурируют фрагментация предложений, избыточная длина предложений, нелогичный порядок фраз и излишне буквальный перевод. Можно выделить несколько более специфических категорий, каждая из которых имеет лингвистическую природу (табл. 2).

Таблица 2

Типология ошибок машинного перевода и их лингвистические последствия

Категория ошибок	Описание и пример	Лингвистическое влияние
Ошибка в словопорядке	Некорректное расположение слов в предложении, особенно характерно для языков с гибким порядком слов	Деградация плавности, искажение синтаксических и семантических отношений
Ошибка в формообразовании	Неправильное склонение или спряжение слова (падеж, число, род)	Снижение адекватности и грамматической корректности, изменение смысла
Лексическая ошибка	Выбор неверного или неуместного слова (неправильный перевод)	Нарушение семантики, создание бессмысленного или "галлюцинирующего" контента
Пропущенные слова	Пропуск слов или частей текста	Снижение адекватности, неполнота смысла
Добавленные слова	Неоправданное включение лишних слов в перевод.	Искажение смысла, снижение адекватности, ухудшение стилистики

Ошибки в словопорядке представляют собой неверное расположение слов. Они являются особенно проблематичными для морфологически богатых языков, например для русского, который обладает гибким порядком слов и сложной падежной системой. Машина может не сохранять корректные грамматические и семантические связи внутри предложения. Ошибки формообразования появляются, когда слово неправильно изменяется (по падежу, числу, роду, времени). Сложные флективные системы многих языков, которые передают смысл, упускаемый при простом подходе «слово за словом», выступают постоянным вызовом. Лексическая ошибка подразумевает выбор неверного или неуместного слова. Подобное обстоятельство может приводить к плавным, но семантически пустым или полностью неверным переводам, способствуя упомянутому ранее феномену «галлюцинации». Анализ также показывает, что пропущенные или добавленные слова являются распространенными причинами

расхождений в переводах, поскольку словарь, которым располагает машина, может не совпадать с тем, что выберет человек [4. С. 61-71].

НМП-системы не просто повторяют недочеты своих предшественников; они создают свой собственный профиль ошибок. Если старые системы могли оставлять слова без перевода или создавать синтаксически неуклюжие результаты, то НМП, в силу своей ориентированности на плавность, склонен создавать грамматически верные, но семантически ущербные предложения. В связи с названной причиной характер задачи постредактирования меняется с простого исправления на кропотливое восстановление смысла. Если предыдущие системы делали ошибки, которые было легко обнаружить, например, непереведенные слова или сломанный синтаксис, то НМП создает грамматически корректную оболочку для своих ошибок. Например, перевод простого приказа.

Take heed of your own souls (рус. «Внимайте своим собственным душам») выглядит правдоподобно, но является полностью неверным для исходного текста. Подобная ошибка является более коварной, поскольку может ввести в заблуждение пользователя и требует более высокого уровня когнитивных усилий от постредактора для обнаружения и исправления семантического несоответствия.

Критически важным вопросом остается, как следует оценивать результат НМП. Окончательным критерием качества является перевод, выполненный человеком. Экспертная оценка признана «золотым стандартом», поскольку специалисты могут использовать знания естественного языка и мира для вынесения тонких суждений, недоступных для автоматических метрик. Однако экспертная оценка затратна, требует много времени и подвержена субъективности и расхождениям между разными оценщиками. Для преодоления ограничений человеческого суждения в этой области были разработаны многочисленные автоматические метрики. Традиционные метрики, такие как BLEU и METEOR, основываются на лексическом сходстве и совпадении n-грамм с эталонным переводом, созданным человеком. Хотя они широко используются благодаря простоте и независимости от языка, у них имеются известные недостатки. Например, BLEU основан на точности, а потому может присвоить высокий балл короткому, плавному, но неточному переводу. METEOR, в свою очередь, пытается улучшить данный подход, включая стемминг, сопоставление синонимов и штраф за изменение порядка слов, демонстрируя несколько лучшую корреляцию с человеческими суждениями. Область лингвистики движется к нейросетевым метрикам, например BLEURT и COMET, которые обучены коррелировать с человеческими оценками и показывают более высокую эффективность, чем их традиционные предшественники [1. С. 1879-1887].

Метрики, используемые для оценки эффективности НМП, часто измеряют то, что удобно с вычислительной точки зрения, а не то, что значимо с лингвистической. Существует фундаментальное несоответствие между статистическим баллом системы и ее подлинным лингвистическим качеством. Тот факт, что НМП может производить очень плавные, но бессмысленные переводы и все равно получать хороший балл по *n*-граммной метрике вроде BLEU, демонстрирует критический недостаток в процессе оценивания. Данные метрики, будь

они основаны на лексическом совпадении или на нейронных эмбеддингах, являются статистическими показателями качества, а не его прямым измерением. Они не могут уловить истинную семантическую точность, культурную уместность или нюансы, необходимые для высококачественного перевода. Данный парадокс указывает на устойчивую цикличность в области: системы «черного ящика» оцениваются метриками «черного ящика», а конечные арбитры качества – переводчики-люди – остаются задействованы в отдельном, менее масштабируемом процессе.

Развитие НМП не привело к устареванию профессии переводчика, но коренным образом изменило его роль. В центре внимания теперь не создание перевода с нуля, а постредактирование результата, сгенерированного машиной. Подобная новая задача во многих случаях оказывается более эффективной по сравнению с традиционным переводом, выполненным человеком. Однако взаимоотношения между человеком и машиной остаются сложными. У переводчиков разные впечатления от постредактирования, а когнитивная нагрузка при подобной работе может быть значительной. Необходимость деконструировать и исправлять плавный, но неверный результат системы требует нового набора навыков и повышенной бдительности. Машина также может воспроизводить предвзятость, присутствующую в ее обучающих данных, что возлагает на человека этическую ответственность за исправление вредных стереотипов.

В конечном счете, НМП-системы преуспевают в работе с большими объемами данных и могут обеспечивать поразительную плавность, но им не хватает способности к подлинному когнитивному пониманию, культурной осведомленности и логическому рассуждению. Профессионалы-лингвисты необходимы для обеспечения контекстной точности, интерпретации нюансов, выполнения сложных аналогий и поддержания общей логической связности и стилистического богатства переведенного текста. Постоянное участие человека в процессе обеспечивает ключевой уровень оценки, согласованный с человеческим восприятием, который не может быть воспроизведен ни одной автоматической метрикой.

Заключение. Траектория развития НМП указывает на будущее, в котором взаимоотношения между машиной и лингвистом будут не конкурентными, а симбиотическими. Машина будет выполнять рутинные, объемные задачи, в то время как человек будет осуществлять незаменимый, тонкий, творческий и критический контроль, который пока остается недоступным для вычислений [6]. Осознание сильных и слабых сторон системы, обусловленных ее внутренней архитектурой, приводит к выводу, что наиболее эффективная модель работы в будущем – совместная. Роль переводчика возвышается от простого «мастера слова» до критического валидатора и носителя культурных и контекстуальных знаний. Именно подобный целостный взгляд на проблему является основным результатом анализа, который начинается с предпосылки, что понимание области находится еще на начальном этапе. Истинная научная основа для НМП возникнет из более глубокого, совместного взаимодействия между исследователями в области машинного обучения и теоретическими лингвистами, с целью демистификации «черного ящика» и установления надежной, общей основы для данной области.

Список литературы

1. Алюнина Ю. М. Возможности и ограничения нейросетевого машинного перевода // XV Конгресс МАПРЯЛ: Избранные доклады [Электронный ресурс] / редкол.: Н. А. Боженкова, С. В. Вяткина, В. Н. Климова и др.; отв. ред. М. С. Шишков. СПб.: МАПРЯЛ, 2024. С. 1879–1887.

2. Дубовикова Е. М., Егоров Г. Г. Использование современных нейросетей при изучении английского языка // Цифровые технологии и право: сборник научных трудов III Международной научно-практической конференции, г. Казань, 20 сентября 2024 г. / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило [и др.]. В 6 т. Т. 3. Казань: Издательство «Познание» Казанского инновационного университета, 2024. С. 246–250.

3. Дубовикова Е. М., Егоров Г. Г. Особенности интерпретации норм англосаксонского права в РФ // Стратегия развития гражданского права в поисках ответов на вызовы XXI века (формы противодействия внешним угрозам): материалы III Международной научно-практической конференции, г. Волжский, 3 декабря 2024 года / отв. за выпуск Г. Г. Егоров; Волжский филиал Федерального государственного автономного образовательного учреждения высшего образования «Волгоградский государственный университет». Москва: Сфера, 2025. С. 37–53.

4. Егоров Г. Г., Севостьянов М. В., Шубенкова К. В. Нормативно-правовое интерпретирование систем на основе «искусственного интеллекта» и нейронных сетей (международные аспекты) // Legal Concept = Правовая парадигма. 2025. Т. 24, № 1. С. 61–71. DOI: https://doi.org/10.15688/lc.jvolsu.2025.1.9

5. Парфенова М. В., Егоров Г. Г. Особенности использования в педагогической деятельности систем на основе машинного интеллекта // Alma mater = Вестник высшей школы. 2025. № 4. С. 70-75. DOI: 10.20339/AM.04-25.070.

6. Bakhteev D.V. Ethical-Legal Models of the Society Interactions with the Artificial Intelligence Technology // Journal of Digital Technologies and Law. 2023. 1(2). P. 520–539. https://doi.org/10.21202/jdtl.2023.22. EDN: ekeudk

УДК 34.03

Д. А. Казанцев,
кандидат юридических наук,
член Совета ТПП РФ
по развитию системы закупок

Искусственный интеллект и законодательный процесс: есть ли пространство для синергии?

Аннотация. Законотворчество – одна из важнейших сфер приложения юридического знания. При этом уже сегодня нейросеть является повседневным инструментом юриста. Ее механистическое внедрение в законодательные процессы создает угрозу и для качества принимаемых нормативных актов. Что еще важнее, бесконтрольное использование технологий ИИ в законодательстве создает угрозу для существования и надлежащего функционирования всей системы права. А значит, не отрицая удобства ИИ как вспомогательного инструмента, важно осмыслить, постулировать и установить принципы и границы его использования в работе юриста в целом и в законодательном процессе в частности.

Ключевые слова: право, цифровые технологии, законотворчество, нейросеть, искусственный интеллект, правопонимание, законодательство

D. A. Kazantsev,
candidate of Legal Sciences,
Member of the Council of the Chamber of Commerce and Industry of the Russian Federation for the Development of the Procurement System

Artificial intelligence and the legislative process: search for synergy

Abstract. Lawmaking is one of the most important areas of application of legal knowledge. At the same time, today the neural network is an everyday tool for a lawyer. Its mechanical introduction into legislative processes poses a threat to the quality of adopted regulations. What is more important, the uncontrolled use of AI technologies in legislation poses a threat to the existence and proper functioning of the entire legal system. Therefore, without denying the convenience of AI as an auxiliary tool, it is important to comprehend, postulate and establish the principles and boundaries of its use in the work of a lawyer in general and in the legislative process in particular.

Keywords: law, digital technologies, lawmaking, neural network, artificial intelligence, legal understanding, legislation

Введение. Все более широкое использование различных технологий т. н. «искусственного управления» в самых разных хозяйственных и бытовых сферах и проникновение этих технологий в государственное и бизнес-управление заставляет взглянуть на них как на фактор управления и регулирования. В известной степени касается это и правового регулирования.

Уже сегодня нейросеть является одним из инструментов работы юриста, а IT-компании соревнуются в разработки ИИ-ассистентов для юридической работы. И хотя полноценные роботы-юристы все еще остаются уделом фантастики, а не практики, но уже сегодня некоторые исследователи выдвигают мысль о том, что «Большие данные могут регулировать и оттачивать разработку правовых норм. Юристам следует уже сейчас разрабатывать нормы, регулирующие ситуации, когда автономные алгоритмы смогут дополнить и заменить человеческое усмотрение в определении оптимальных правовых норм и сумеют находить соответствующие различия между людьми и использовать их для персонализации санкций, прав и обязанностей» [7. С. 17].

Такая формулировка проблематики обозначает не только перспективу, но и в первую очередь угрозу личности и реальным правам, свободам и возможностям человека в цифровизирующемся обществе. И одним из неочевидных, но оттого не менее существенных рисков, связанных с использованием ИИ в правовом поле, является внедрение его в законодательный процесс.

В крайнем выражении такой риск заключается в делегировании искусственному интеллекту полномочий законотворчества от составления законопроекта до анализа целесообразности его принятия. По счастью, сегодня реализация такого «цифрового законотворчества» на практике всерьез не обсуждается. Но даже частичное внедрение ИИ в законотворчество без должной проработки и жестких ограничений далеко не безопасно. Делегирование даже самой развитой нейросети полномочий законодателя или правоприменителя создает угрозу выхолащивания самой сути права.

Вместе с тем «появление новых общественных отношений в условиях цифровой реальности приводит как к трансформации самого права, становящегося объектом цифровизации, так и к обновлению статуса личности» [6. С. 94]. Возможна ли такая трансформация как без крайности отрицания технологического прогресса, так и без крайности правового нигилизма, превращающего правовые нормы не более чем в еще один источник «больших данных» для нейросети?

Представляется, что на принципиальном уровне достижение такого баланса возможно. Но для его достижение необходимо постулирование и соблюдение нескольких принципиально важных принципов внедрения и использования нейросети в области правотворчества.

Основная часть. Прежде всего, стоит вновь и вновь постулировать отсутствие у нейросети, как и у любой другой системы искусственного интеллекта, статуса правового субъекта. На сегодня можно констатировать «несостоятельность предложения признания за искусственным интеллектом правосубъектности, аналогичной правосубъектности физического лица, и, несмотря на использование принципов работы человеческого мозга для построения системы искусственного интеллекта, принципы правового регулирования статуса физического лица не могут быть применены к искусственному интеллекту» [3. С. 33].

Рассуждение о роли нейросети в законодательном процессе базируется на этом постулате, хотя и не ограничивается им. Помимо отсутствия статуса правового субъекта у ИИ, необходимо помнить еще и о том, что превосходство ИИ

над человеком в части объемов и скорости обработки информации не снимает вопроса о качестве ее обработки.

Речь идет не только и не столько о пресловутом «галлюцинировании», сколько о том, что обработка информации нейросетью объективно лишена гуманитарного измерения. Не потому, что нейросеть недостаточно совершенна. А потому, что на принципиальном уровне ее задача в другом. Задача нейросети – не заменять человека, а работать в тех условиях, в которых работа человека невозможна.

Право же как социальный феномен по самой свой сути антропоцентирчно. Оно возникало и развивалось как инструмент регулирования отношений между людьми в сообществе людей. Иные биологические субъекты – например, животные, в т. ч. высшие приматы – даже будучи включены в круг объектов правового регулирования, не становятся его субъектами.

Частым следствием этого является тот факт, что уровень и характер развития права отражает уровень и характер общественного развития. Именно общественного, а не научно-технического. А потому для решения вопроса о правовой субъектности ИИ ключевое значение имеет не его техническое совершенство, а уровень его гуманизации.

И эта проблематика предопределяется онтологическими характеристиками искусственного интеллекта. Довольное точное и все еще актуальное определение ИИ дано в Указе Президента России, посвященном развитию искусственного интеллекта: «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека» [1]. Результаты интеллектуальной деятельности в части сбора и обработки информации уже качественно превосходят способности человека, но вот сами методы обработки все еще являются именно имитацией когнитивной деятельности человека.

В развитых моделях ИИ сегодня внешние выражения обработки информации – ответы на вопросы, понимание контекста, ирония и тому подобное – и в самом деле обнаруживают черты сходства с мышлением человека. Но важно помнить: сходство само по себе не означает тождества.

В этом и именно в этом контексте актуальна мысль о том, что «подходы, которые предлагают обосновать правосубъектность роботов и ИИ с учетом сущности одушевленных субъектов, у которых есть реальная, а не только формально-юридическая воля, получат развитие только после того, как развитие цифровых технологий достигнет объективно высокого уровня» [2. С. 36]. И уровень этот определяется не только количественными показателями в части обработки информации, но и наличием мышления, схожего с мышлением человека.

Вдвойне важен этот аспект для законодательства. Ведь любой качественный закон исходит не только из формального равенства субъектов и следования остальным правовым постулатам, но и из необходимости исправить правовым регулированием ситуации фактического неравенства. Если угодно «скорректировать» общественные отношения там, где без корректировки они могу разви-

ваться по пути, создающему угрозу для личности и общества. Именно в этом, а вовсе не в формулировке отдельных норм, состоит подлинное искусство законодателя.

Искусственный интеллект сегодня не может ни подменить собой законодателя, ни даже принять на себя его функции в отдельных отраслях. Означает ли это принципиальную невозможность участия ИИ в законотворчестве? Отнюдь не означает. Вот только ИИ необходимо рассматривать не как замену законодателю, а как помощника для него. Притом помощником со строго ограниченными функциями в строго определенных областях.

Правоведом и сегодня, и в обозримой перспективе может быть лишь человек. Да и то далеко не заурядный человек, а лишь обладающий не просто соответствующим комплексом знаний, в котором глубокое понимание теории находится в гармонии с практикой, но и имеющий высокий уровень культуры мышления. Если мы говорим о законотворчестве именно как о создании правового закона, то есть о позитивной фиксации объективным правовых норм, то в отсутствие специфической научно-правовой квалификации законотворчество невозможно.

А потому ИИ сегодня может при определенных условиях успешно имитировать законотворчество. Он уже может делать это быстрее, чем биологические разработчики законопроектов. ИИ даже может превзойти их по части юридической техники – и текст, похожий на закон, будет еще и приятен для чтения. Вот только даже в этом случае он все еще не будет законом.

«Возможно использование ИИ для разработки рутинного законодательства. Но нельзя исключать технические ошибки или уязвимости в программах ИИ: ошибки или недочеты в алгоритмах могут привести к ошибкам в составлении законопроектов, противоречиям между статьями или непредвиденным последствиям» [9]. То есть нейросеть успешно формулирует норму или несколько норм. Но хороший закон – это куда больше, чем совокупность норм.

Максимально упрощая, можно с уверенностью утверждать: ИИ может написать дурной закон лучше человека. Но вот для того, чтобы сделать хороший закон, человек все же необходим. Более того, необходим целый консилиум специалистов. Означает ли это то, что для нейросети в законотворчестве нет места? Вовсе не означает! Но критически важно определить для нее область эффективного применения.

Это, в сущности, ровно та область, для которой ИИ создавался изначально: область обработки больших объемов стандартизированной информации без ее интерпретации. В области законотворчества речь идет об имплементации работы ИИ в те стадии законодательного процесса, которые не связаны с принятием решения, но необходимы для подготовки такого решения. Тот же подход, пусть и с известной корректировкой, можно применить и более широко – не только к законотворчеству, но и к нормотворчеству вообще. Более того, на практике именно в отдельных областях незаконодального нормотворчества апробировать и обучать ИИ целесообразнее всего.

И такое апробирование на практике уже происходит. Происходит всякий раз, когда недостаточно квалифицированный или просто очень занятый юрист

прибегает к помощи нейросети. И сфера законодательства от этого вовсе не застрахована. «Независимо от того, будет ли это иметь положительный или отрицательный эффект, законодательство, созданное с помощью ИИ, неизбежно – этого требует растущая сложность политики. Для этого не нужно вносить изменения в законодательные процедуры или получать согласие какого-либо комитета по правилам. Достаточно, чтобы один помощник законодателя или лоббист запустил чат-бота» [8].

Запрет на использование нейросетей в законодательном процессе возможен технически, но едва ли реализуем на практике. А значит, куда эффективнее политики запретов может быть политика регулирования и локализации применения ИИ в законотворчестве.

Например, при внесении законопроекта в парламент, но до направления его текста в профильные комитеты, можно поручать ИИ проведения анализа гармонизации предлагаемых норм законопроекта с нормами действующего законодательства. При выявлении потенциальных противоречий ИИ составляет отчет со ссылками на конкретные пункты и подпункты тех нормативных актов, которым принимаемый законопроект может противоречить.

И здесь важно подчеркнуть: наличие такого отчета не должно будет означать возвращения законопроекта на доработку. Ведь для противоречия могут быть и объективные причины. Например, ИИ обнаружил мнимые противоречия в сходном по терминологии нормативном акте, предназначенном для регулирования отношений в иной сфере (допустим, законопроект касается изменения требований к проведению электронного аукциона по Закону № 223-ФЗ «О закупках», а противоречие выявлено с нормами об электронном аукционе, содержащимися в Законе № 44-ФЗ «О контрактной системе»). Или мнимое противоречие может быть выявлено между общими и специальными нормами (а мы помним, что «специальный закон отменяет действие основного»). В конце концов, такой отчет не имеет 100 % страховки от проникновения в него уже упомянутых выше галлюцинирований.

Что же делать с таким отчетом? Субъект законодательной инициативы прорабатывает такой отчет и дает комментарий по каждому его пункту. При необходимости он исключает из текста законопроекта спорные формулировки. Однако замечание, включенное в отчет ИИ, не создает обязанности по корректировки законопроекта.

После этого законопроект поступает в профильные комитеты вместе с отчетом и комментариями к нему. И для профильных комитетов этот документ служит именно ориентиром, а не руководством к действию по части критики законопроекта.

В той же мере полезным – и в той же самой мере рекомендательным – может быть прохождение лингвистической экспертизы законопроекта с помощью инструментов ИИ перед его третьим чтением. Нейросеть уже сегодня способна подсказать автору более лаконичные, более ясные, а иногда и более точные формулировки. Но лишь законодателю решать вопрос о том, уместные ли предложенные искусственным интеллектом формулировки в данном конкретном законопроекте.

Те же потенциальные возможности ИИ могли бы пригодиться не только при принятии законов, но и в еще большей степени – при разработке подзаконных НПА. А еще до внедрения в область разработки ведомственных актов ИИ будет апробирован при создании локальных нормативных актов хозяйствующих субъектов.

Однако законодательная деятельность не ограничивается лишь изданием новых документов. Важнейшей компонентой является систематизация документов, уже вступивших в силу. Подчас же для серьезного юридического анализа необходимо и привлечение норм документов, утративших свою силу полностью или частично. Подобная систематизация служит не только снижению трудоемкости и повышению точности работы юристов, но и общей популяризации права.

Стандарты такой систематизации в России уже заданы коммерческими справочными правовыми системами. Ни одну из них пока что нельзя назвать безупречной, но именно их интерфейсные и архитектурные решения вполне можно использовать при разработке официального электронного свода российского законодательства.

Состав такого свода – предмет отдельного и содержательного исследования. Здесь же стоит кратко обозначить то, что в нем непременно необходимо учесть не только действующие и утратившие силу узаконения Российской Федерации, но и документы советского периода, и, конечно же, доступные для оцифровки документы дореволюционной эпохи (включая Свод законов Российской империи, но не ограничиваясь им). В числе документов должны фигурировать не только законы и подзаконные акты, но и судебные решения, монографии ведущих законоведов и даже максимально возможный круг публикаций юристов в профессиональной периодике.

Заключение. Использование ИИ в правовой сфере – это уже не перспектива, а реальность. Представляется, что его использование в этой сфере с каждым годом будет лишь расширяться.

«Алгоритмы и искусственный интеллект найдут применение в публично-правовых отношениях. Такое применение должно основываться на глубоком теоретическом осмыслении, технических и социальных расчетах, на учете имеющегося опыта, в том числе ошибочного. Очевидно, что от алгоритмов, примененных искусственным интеллектом, способны пострадать фундаментальные права человека – равенство, право на частную жизнь и защиту персональных данных, право на судебную защиту против решений, принятых алгоритмом» [5. С. 39].

Однако есть основания для надежды на то, что роботизированное законодательство не подменит собой подлинное нормотворчество, а робот останется ассистентом юриста и не станет его конкурентом.

Для этого уже сегодня необходимо осмысление значения, роли и места цифровых технологий в правовой среде с привлечением теоретико-правового инструментария и достижений философии право. Ведь при проработке вопроса о степени допустимого внедрения нейросети в законодательный процесс долж-

ное правопонимание из отвлеченный, на первый взгляд, теории становится фактором обеспечения безопасности развития общества.

«Одной из задач современного правоведения представляется выявление условий для <…> сужение поля псевдоправовой мифологии, порождаемой надеждами на чудодейственный потенциал новых технологий, якобы способных создать новую парадигму правоотношений. Видимо, предстоит критически пересмотреть ценностные ориентиры современного права и, не отрицая нормативно-позитивистского подхода, обратить большее внимание на социальные, нравственные и культурные основания права – своего рода интеллектуальное завещание С. С. Алексеева, Г. В. Мальцева, В. С. Нерсесянца и других выдающихся правоведов» [4. С. 18].

А значит, популяризация и расширение знаний о праве – это залог конструктивного и безопасного развития синергии социума и цифровых технологий [10–14]. Такая синергия принципиально достижима. Но для ее достижения требуется не разовая, а регулярная проработка методов и схем взаимодействия человека с цифровыми инструментами. И сфера законотворчества представляет собой важный, но далеко не единственный пример выстраивания подобного взаимодействия. Некоторые ключевые аспекты компьютеризированных инноваций могут быть реализованы только с помощью методов и процедур, определенных нормативными актами. Подобные нормативные акты еще не приняты, и существует вероятность, что в ближайшее время они не будут приняты, что может подорвать полноценное внедрение цифровых инноваций [10. С. 27].

Список литературы

1. О развитии искусственного интеллекта в Российской Федерации: Указ Президента России от 10.10.2019 № 490 (в ред. от 15.02.2024) // СПС «ГАРАНТ». URL: https://base.garant.ru/72838946/ (дата обращения: 05.09.2025).

2. Бегишев И. Р. Искусственный интеллект и робот как правовые категории // Безопасность бизнеса. 2020. № 6. С. 32–36.

3. Дурнева П. Н. Искусственный интеллект: анализ с точки зрения классической теории правосубъектности. Гражданское право. 2019. № 5. С. 30–35.

4. Ковлер А. И. Антропология прав человека в цифровую эпоху (опыт сравнительного анализа) // Журнал российского права. 2022. № 12. С. 5–29.

5. Талапина Э. В. Алгоритмы и искусственный интеллект сквозь призму прав человека // Журнал российского права. 2020. № 10. С. 25–39.

6. Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. №1. С.93–98.

7. Харитонова Ю. С., Ци Сунь. Верховенство закона и алгоритмизация принятия решений в России, Китае, Европе // Право и бизнес. 2023. № 2. С. 11–17.

8. Nathan Sanders, Bruce Schneier. AI Will Write Complex Laws // Lawfare, 2025. URL: https://www.lawfaremedia.org/article/ai-will-write-complex-laws (дата обращения: 29.08.2025).

9. Ylenia Maria Citino. Bot-Legislator and AI-powered legislative processes // MediaLaws, 2025. URL: https://www.medialaws.eu/bot-legislator-and-ai-powered-legislative-processes/ (дата обращения: 25.08.2025).

10. Ндиюн Р. К., Муконза Р. М. Цифровая трансформация системы регистрации актов гражданского состояния Камеруна: инновации в электронном управлении // Journal of Digital Technologies and Law. 2025. Т. 3, № 1. С. 7–34. https://doi.org/10.21202/jdtl.2025.1. EDN: eaqyqj

11. Казанцев, Д. А. Правовые механизмы распределения ответственности за вред, причиненный системами искусственного интеллекта / Д. А. Казанцев // Journal of Digital Technologies and Law. 2025. Т. 3, № 3. С. 446–471. DOI 10.21202/jdtl.2025.18. EDN RUZMXP.

12. Казанцев, Д. А. Использование искусственного интеллекта для проведения конкурентных закупок: проблемы правового регулирования / Д. А. Казанцев, П. Догнал, П. П. Догнал // Journal of Digital Technologies and Law. 2024. Т. 2, № 3. С. 585–610. DOI 10.21202/jdtl.2024.30. EDN DLADNS.

13. Казанцев, Д. А. Проблемы и перспективы регулирования отношений в рамках сделки, совершенной с участием искусственного интеллекта / Д. А. Казанцев // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 438–463. DOI 10.21202/jdtl.2023.18. EDN JYQAZW.

14. Казанцев, Д. А. Авторские права на результаты деятельности искусственного интеллекта и способы их защиты / Д. А. Казанцев // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 909–931. DOI 10.21202/jdtl.2023.39. EDN PHBNKI.

УДК 349.2

А. Г. Авдей,
кандидат юридических наук, доцент,
Гродненский государственный университет
имени Янки Купалы

О дифференциации гражданских и трудоправовых отношений в платформенной занятости

Аннотация. Процессы глобализации и регионализации обусловили появление нетипичных форм занятости. Занятость на цифровых платформах – объективная реальность настоящего времени. Для регламентации исследуемых отношений очевидно применение инструментов трудового и гражданского права. Выделяются основные признаки для разграничения гражданских и трудоправовых отношений в условиях занятости на цифровых платформах. Платформенная занятость требует самостоятельного, отдельного правового регулирования, учитывая ее гибкость, цифровое отражение природы и алгоритмическое управление.

Ключевые слова: право, платформенная занятость, цифровая платформа, правоотношения, цифровые технологии, трудовые отношения, нетипичные формы занятости

A.G. Audzei,
Candidate of Law, Associate Professor,
Yanka Kupala State University of Grodno

On the differentiation of civil and laboratory relations in platform employment

Abstract. The processes of globalization and regionalization have led to the emergence of atypical forms of employment. Employment on digital platforms is an objective reality of the present time. To regulate the relations under study, it is obvious to use the instruments of labor and civil law. The main features for distinguishing civil and labor relations in the context of employment on digital platforms are highlighted. Platform employment requires independent, separate legal regulation, given its flexibility, digital reflection of nature and algorithmic management.

Keywords: law, platform employment, digital platform, legal relations, digital technologies, labor relations, atypical forms of employment

Введение. В Беларуси уделяется большое внимание развитию цифровых технологий. В настоящее время завершается реализация государственной программы «Цифровое развитие Беларуси 2021–2025 годы» и идет работа над

Стратегией цифрового развития страны на следующее пятилетие. Отметим, что важным шагом, в контексте цифровизации республики, является реализация Концепции обеспечения суверенитета в сфере цифрового развития до 2023 года, утвержденной постановлением Совета Министров Республики Беларусь от 31 декабря 2024 г. № 1074. Платформенная занятость является одним из компонентов современного рынка труда Беларуси с использованием ресурсов цифровых платформ. Без эффективного законодательного регулирования исследуемого вида занятости, невозможен унифицированный подход к использованию платформ и информационных технологий, а также оперативное реагирование на возникающие трудности в области цифрового развития.

Основная часть. Разделяем существующее в доктринальных источниках мнение о том, что «природа платформенной занятости остается одной из самых дискуссионных тем в современной науке трудового права последний лет» [1. С. 120]. Унифицированного подхода к правовому регулированию исследуемой нетипичной формы занятости не существует в зарубежной практике. Для регламентации платформенной занятости очевидно применение инструментов как трудового, так и гражданского права.

Подмена трудовых отношений гражданско-правовыми отношениями острая тема, особенно в контексте социальной защиты занятых на цифровых платформах, учитывая изменения в Закон Республики Беларусь от 15 июля 2021 г. № 118-З «О взносах в бюджет государственного внебюджетного фонда социальной защиты населения Республики Беларусь», которые вступили в силу 18 августа 2025 года.

Среди риск маркеров, с которыми операторы цифровых платформ, могут столкнуться для разграничения трудовых и гражданско-правовых отношений в условиях нетипичной занятости можно выделить следующие:

1. Трудовая терминология. В договоре использованы термины: работник, вместо исполнитель; наниматель, вместо заказчика и т. д.

2. Одинаковая ежемесячная оплата, что демонстрирует тот факт, денежное вознаграждение не зависит от результата работы, а от процесса.

3. Сроки выплат совпадают с выплатой штатным работникам.

4. Отсутствие в договоре условия о результате конкретных работ. В частности, нет четкой формулировки того, что ожидается по итогу занятости: результат или процесс.

5. Установление режима работы. В договоре указано формально или фактически время работы, что демонстрирует зависимость и подчинение оператору цифровой платформы, который фактически выступает в роли нанимателя.

6. Единственный источник доходов занятого от цифровой платформы, а не от иных субъектов, которым оказываются услуги, как при гражданско-правовой регламентации отношений.

7. Отсутствие рисковых условий в договоре (неустойка, штраф и т. д.), которые имеют место быть в гражданских правоотношениях.

8. В договоре закреплены трудоправовые гарантии (отпуск, выходные дни и др.).

Заключение. Важным моментом разграничения трудовых и гражданско-правовых отношений занятости на цифровых платформах является то, что трудовые отношения строятся на власти и подчинении, а не на отношениях равенства и предпринимательского риска. Думается, что при наличии хотя бы нескольких признаков трудовых отношений при платформенной занятости, они должны быть презюмируемо признаны таковыми.

Специфика платформенной занятости требует разработки и принятия Закона Республики Беларусь «О платформенной занятости», который будет иметь комплексный межотраслевой характер, на основе лучших зарубежных практик с учетом национальных интересов.

Список литературы

1. Мотина Е. В. Правовое регулирование нетипичных форм занятости в условиях цифровизации и региональной интеграции: [монография] / Е. В. Мотина, К.Л. Томашевский, Е.В. Чичина. Минск: Амалфея, 2024. 243 с.

УДК 342

Е. И. Дискин,
кандидат юридических наук, старший научный сотрудник,
Национальный исследовательский университет
«Высшая школа экономики»

Новые подходы к регулированию информационного перенасыщения, формируемого цифровыми платформами

Аннотация. Статья посвящена правовым аспектам регулирования информационного пространства в условиях массового распространения «мусорной» и чрезмерно эмоциональной информации в цифровой среде. Анализируются негативные последствия информационного перенасыщения для когнитивной автономии личности, включая снижение способности к концентрации, осмысленному восприятию и критическому мышлению. Особое внимание уделено роли цифровых платформ как ключевых распространителей такого контента. На основе концепции информационной энтропии предлагается правовая модель оценки уровня информационного перегруза, включающая формулу для количественного определения «мусорной» информации. Данная модель может лечь в основу нормативного регулирования объема и качества контента, предлагаемого пользователям. Цель исследования – выработка правовых инструментов, направленных на защиту когнитивного здоровья граждан и обеспечение ответственного управления информационными потоками в цифровом обществе.

Ключевые слова: информационное право, информационное перенасыщение, регулирование цифровых платформ, когнитивное здоровье, мусорная информация, социально-информационная энтропия, полезная информация

E. I Diskin,
Candidate of Law, Senior Research Fellow,
HSE University

New approaches to regulating information overload generated by digital platforms

Abstract. The article focuses on the legal aspects of regulating the information space amid the widespread dissemination of "junk" and highly emotional content in the digital environment. It examines the negative impact of information overload on individuals' cognitive autonomy, including diminished concentration, comprehension, and critical thinking. Special attention is given to digital platforms as primary distributors of such content. Based on the concept of informational entropy, a legal framework is proposed for assessing the level of information saturation, including a formula to quantify "junk" information. This model can serve as a basis for regulatory control over the volume and quality of user-targeted content. The study aims to develop

legal tools to protect citizens' cognitive well-being and ensure responsible management of information flows in the digital society.

Keywords: Digital law, Information overload, Regulation of digital platforms, Cognitive well-being, Junk information, Socio-informational entropy, useful information

Введение. Важным свойством процесса медиапотребления в современном обществе является фактор широкого распространения развлекательной информации, которая не может быть охарактеризована как искусство или акт творчества. Бессмысленные и бесполезные факты о жизни чужих людей (т.н. знаменитостей), которые не несут никакого морального или созидательного смысла, бесконечные короткие ролики, колоссальные потоки рекламы – вряд ли можно всерьез утверждать, что такая информация уменьшает некую неопределенность в жизни человека. Скорее наоборот, она подобно мусору заполняет наше сознание, сокращая нашу способность к созиданию и творчеству, способствуя таким негативным явлениям как прокрастинация, утрата ценностных и моральных ориентиров, приводят к исчезновению живой, неэлектронной коммуникации между людьми [1]. Человек утрачивает способность к концентрации внимания, постоянно отвлекаясь на различные взаимодействия с «мусорной» информацией. Это состояние ярко описал социолог и футуролог Элвин Тоффлер: «нас все больше пичкают короткими модульными вспышками информации – рекламой, командами, теориями, обрывками новостей, какими-то обрезанными, усеченными кусочками, не укладывающимися в наши прежние ментальные ячейки» [6].

Как справедливо отмечают исследователи – человечество сталкивается с информационным перенасыщением, которое вызвано не только обилием ее источников, но и новыми средствами для создания и доставки информации [7]. Важным фактором этого процесса можно назвать проблему «эмоционализации» информации, т. е. насыщение медиа пространства информацией (прежде всего аудиовизуальной), несущей глубокую эмоциональную окраску, а также «стрессовой информации» о различных бедствиях, кризисах, войнах и несчастьях во всех уголках планеты, направленной на то, чтобы вовлекать зрителя в ее бесконечное потребление [7]. В этих условиях «человеческий мозг больше не строит причинно-следственных связей, не хочет анализировать и воспринимать информацию, привыкает к простому инфопотоку с нулевым результатом его усвоения» [3]. На наш взгляд, регулирование оборота информации должно быть направлено на минимизацию данных эффектов, которые на текущий момент, только усиливаются.

Специалисты по нейропсихологии объясняют, что информационное перенасыщение, нередко описываемое через феномен «клипового мышления» связано с объективными процессами физиологии мозговой деятельности, так: «для осознания и осмысления [информации] необходима, исходя из физиологических временных характеристик, активация связей между воспринимающей областью коры и моторной речевой областью через вовлечение таламического механизма фокусированного внимания. Причем активация корковых нейронов – не менее 500 мс, неспецифических ядер таламуса – не менее 300 мс, затем от таламуса

активируются корковые нейроны, т. е. осмысление и осознание – это корково-таламо-корковый механизм со своими заданными природой временными характеристиками. Следовательно, в так называемом клиповом мышлении не происходит закрепление данной информации в акцепторе результатов действия, *что не позволяет обращаться к пережитому жизненному опыту, планировать и прогнозировать собственное поведение в меняющихся условиях среды* (выделено автором)» [2].

Таким образом, информационное перенасыщение представляет собой достаточно серьезную угрозу для когнитивной деятельности человека. Однако, задачи регулирования информационного потока весьма сложны, так как в основе их решения лежит необходимость построения регуляторных конструкций – запретов и рекомендаций в отношении субъектов, организующих распространение информации (поисковых систем, социальных сетей, маркетплейсов) на неких объективных данных. Представляется возможным предложить решение такой задачи путем предложения формулы для вычисления информационного перенасыщения, которая будет являться ориентиром для регулирования цифровых платформ в отношении объема и качества предлагаемой потребителю информации.

Основная часть

Возможные подходы к оценке информационного перенасыщения. В контексте описанной задачи можно использовать категорию неопределенность из теории информационной энтропии Шеннона в целях выработки формулы социально-информационно энтропии, наделив эту категорию несколько иным смыслом. Гипотезой для выработки подходов к ее определению будет предположение о том, что неопределенность сокращается при снижении объема потребляемой «мусорной» и чрезмерно эмоциональной информации. Соответственно неопределенность будет являться мерой социально-информационной энтропии.

Под неопределенностью в данном случае понимается уровень информационной нагрузки на человека. Максимальная неопределенность соответствует максимальному информационному перенасыщению, выраженному в таком уровне давления на перцептивную и когнитивную сферу деятельности нервной системы, при достижении которого, человек под влиянием стресса оказывается временно неспособен получать, осознавать и практически использовать поступающую информацию, т. е. впадать в состояние прострации или испытывать «техно-мозговое выгорание» [9].

Не менее важным является выработка понятия «мусорная» и чрезмерно эмоциональная информация (далее – мусорная). В частности, переход к преобладанию аудиовизуальной информации еще в 1990-е гг. привел к возникновению упомянутого феномена «клипового мышления», которое Т. Н. Горобец и В. В. Королев предлагают именовать «клиповым восприятием», в силу того обстоятельства, что оно не связано с осмыслением информации [2]. Поэтому в первую очередь, мы отнесем к категории мусорной информации аудиовизуальный контент продолжительностью менее 2 минут, среди которых можно выделить такую категорию как «истории» (stories) – длительность которых может достигать 15–30 секунд. Так же к этой категории относится контент в любой

форме, в котором эмоциональная составляющая преобладает над общим смыслом послания. Помимо этого, к такому контенту мы относим скрытую или навязчивую рекламу, информацию сенсационного характера, а также дезинформацию, т.е. информацию, намеренно вводящую в заблуждение. Мусорной информацией предлагается считать коллективные чаты, общение в которых не регламентировано правилами и не подвергается модерации. К этой категории отнесем навязчивые уведомления от сайтов, приложений и платформ, призванные вовлечь пользователя во взаимодействие. Для удобства мы объединили их в табл. 1.

Таблица 1

Виды мусорного контента

Виды мусорного контента (информации)			
№	**Тип мусорной информации**	**Описание**	**Примеры/Особенности**
1	Аудиовизуальный контент короткой продолжительности	Контент продолжительностью менее 2 минут	Короткие ролики в ленте социальных сетей или в описании товаров маркетплейсов
2	«Истории» (stories)	Особая категория короткого аудиовизуального контента, обычно отображаемая над лентой сообщений социальной сети или мессенджера	Длительность до 15 или 30 секунд
3	Эмоционально перегруженный контент	Контент в любой форме, где эмоциональная составляющая преобладает над смыслом, в т. ч. контент основанный на чрезмерной сексуализации, демонстрации агрессивного, асоциального, аморального поведения	Информация, изложенная таким образом, что вызывает немедленную эмоциональную реакцию, часто провокативного характера
4	Скрытая реклама	Реклама, замаскированная под другой тип контента	Нативная реклама, продакт-плейсмент
5	Навязчивая реклама	Агрессивная реклама, мешающая восприятию основного контента	Pop-up реклама, баннеры
6	Сенсационная информация	Информация сенсационного характера	Желтая пресса, новости о бедствиях и происшествиях в далеких странах, не имеющие практического значения для жизни индивида
7	Дезинформация	Информация, намеренно вводящая в заблуждение	Обычно новостная информация на самые обсуждаемые или провокационные темы
8	Нерегулируемые коллективные чаты	Чаты без правил и модерации	Спам, флуд, хаотичное общение
9	Навязчивые уведомления	Уведомления от сайтов, приложений и платформ	Push-уведомления, призывы к взаимодействию

Не менее сложным является выделение «качественного» контента. По нашему мнению, это информация, соответствующая следующим критериям.

Таблица 2

Основные критерии для определения полезной информации

Основные критерии определения полезного контента (информации)	
Приоритет качества над количеством и скоростью потребления	Глубокий по смыслу, структурированный контент
Стремление к достоверности и проверяемости	Изложение контента таким образом, чтобы изложенные факты и сведения были доступны для проверки и основывались на научном знании и экспертной оценке
Практическая ценность и актуальность	Применимость полученной информации в реальной жизни, стремление к повышению ее качества
Этическая и моральная ценность	Контент должен соответствовать этическим и моральным нормам, сложившимся в обществе

Исходя из изложенных вводных и предложенных определений базовых понятий, основываясь на гипотезе о необходимости снижения неопределенности в информационном пространстве индивидуума, представляется возможным предложить формулу для расчета неопределенности, создаваемой мусорной информацией.

U – уровень неопределенности (чем выше – тем больше когнитивной перегрузки, информационного перенасыщения);

I_t – общий объем потребляемой информации за единицу времени;

I_e – объем **мусорной информации;**

$I_s = I_t - I_e$ – объем полезной информации;

$\alpha = I_e / I_t$ – доля эмоциальной и «мусорной» информации;

β – коэффициент влияния мусорной информации на рост неопределенности;

γ – коэффициент снижения неопределенности за счет получения полезной информации.

Возможная формула:

$$U = \beta \cdot I_e - \gamma \cdot I_s = I_t (\beta \cdot \alpha - \gamma \cdot (1 - \alpha))$$

Поскольку достоверных сведений о том, какая доля информации в Сети является «мусорной» нет, мы предлагаем использовать гипотезу о том, что доля такой информации соответствует принципу Парето (правило 80/20) [4], впервые сформулированному итальянским экономистом Вильфредо Парето в 1896 г. Данный принцип демонстрирует устойчивое неравномерное распределение причин и следствий в различных системах. В частности, мы предлагаем исходить из того, что 20 % потребляемой информации дают 80 % полезных знаний. Таким образом, если наша гипотеза о применимости принципа Парето к потреблению информации верна – 80 % получаемой информации является мусорной.

Исходя из предложенной нами формулы, можно определить оптимальный уровень потребления информации, который будет обеспечивать максимальный уровень полезности и не создавать перегрузку когнитивной сферы человека.

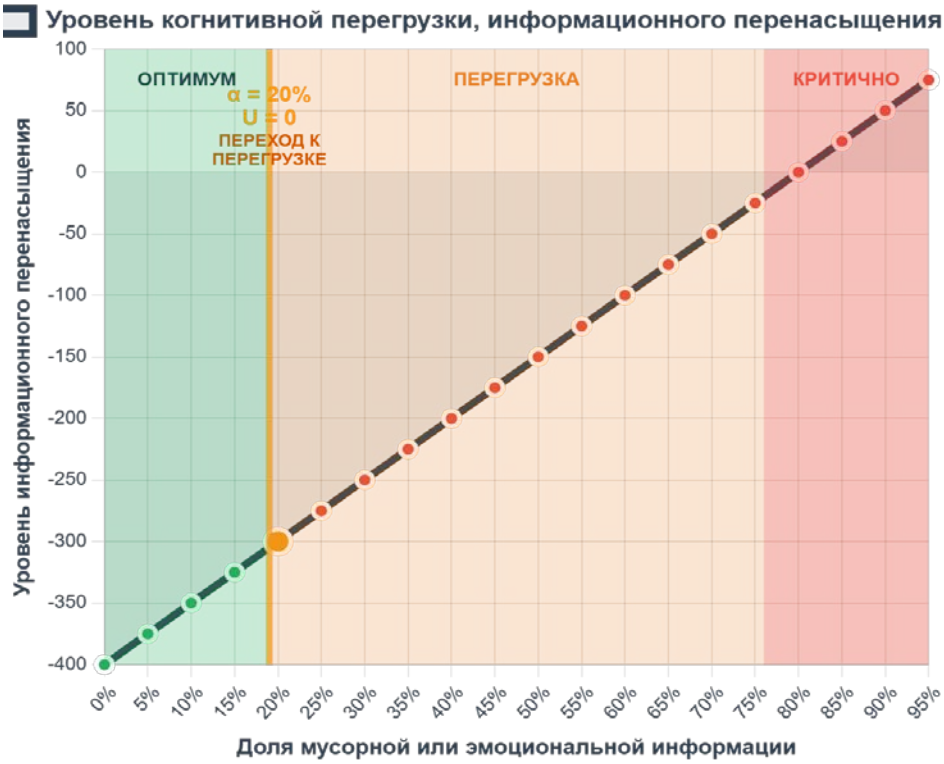


Рис. 1. График зависимости потребления мусорной информации к уровню когнитивной перегрузки или информационного перенасыщения

В соответствии с распределением Парето γ (коэффициент снижения неопределенности за счет получения человеком полезной информации) будет равен 4β (коэффициент влияния мусорной информации на рост неопределенности). Это означает, что одна единица полезной информации способна «перевесить» четыре единицы информационного мусора.

Если попытаться проиллюстрировать это на примере, то если из 10 новостных сообщений: 2 – «мусор», а 8 – глубокая аналитика, будет достигнут условно «правильный» баланс потребления информации, который не будет приводить к когнитивной перегрузке.

Заключение. Безусловно, данная формула не является продуктом глубокого эмпирического исследования медиапотребления, более того, мы сознательно избегаем привычной для исследователей медиапотребления методологии, в которой происходит деление источников, видов и каналов распространения информации, выделения возрастных групп и т. д. В данном случае мы предпринимаем попытку максимального обобщения всех видов и каналов информации в Сети, т. е. анализируем то, что видит и читает человек с экрана смартфона, компьютера или планшета каждый день без сегментации по видам и типам приложений. Мы исходим из того, что общую информационную перегрузку дает совокупное использование Интернета – будь то сайты или приложения. Соответ-

ственно, считаем целесообразным исходить из необходимости снижения объема потребления мусорной информации от всех видов источников информации. При этом мы отдаем себе отчет, что социальные сети и аудиовизуальные сервисы, а также мессенджеры лидируют в совокупном объеме цифровой информации, получаемой современным пользователем.

Можно также согласиться с замечанием о том, что применение принципа Парето недостаточно обоснованно с точки зрения эмпирического измерения медиапотребления, однако есть косвенные данные, которые позволяют говорить о том, что в условиях дефицита соответствующих измерений, распределение соблюдается. Разумеется, с определенной погрешностью, однако не такой большой, чтобы отказываться от его применения. Например, согласно одному из опросов, 68,3 % россиян заходят в Интернет, чтобы получать «актуальные новости и быть в курсе событий». В самом желании нет ничего предосудительного, но при этом в среднем они проводят в Сети 8 часов в день [5]. Если говорить о населении Земли в целом, то мы предлагаем обратить внимание на следующие цифры: пользователи чаще всего используют мессенджеры и социальные сети (94 %). Образовательные сайты и приложения – только 23,8 % [8].

Таким образом, приведенная формула – полезная первая аппроксимация, призванная повысить качество регулирования и показать, на каких принципах и вводных данных оно может строиться. В данном случае, ключевой задачей является поиск баланса между полезной и мусорной информацией. Полагаем, что введение в оборот формулы когнитивной перегрузки будет полезно для последующих изысканий в данной области. Это может быть полезно для регулирования рекламы, модерации контента, потребления информации детьми и подростками и в других регуляторных сценариях.

Список литературы

1. Бушуева А.А., Репринцева Е.А. Компьютерные игры детей: от порождаемых компьютером страхов – к педагогическому сопровождению социально-нравственного развития младших школьников // Психол.-пед. поиск. 2012. № 2(22). С. 125–134.

2. Горобец Т.Н., Ковалев В.В. «Клиповое мышление» как отражение перцептивных процессов и сенсорной памяти // Мир психологии. 2015. № 2 (82). С. 94–100.

3. Коробова О.В., Егорченкова Н.Б., Басс, Е.В. Информационная культура личности в условиях информационного перенасыщения // Феноменология личности: ресурсность и многоаспектность: Сборник материалов Всероссийской научно-практической конференции, Армавир, 22 ноября 2022 г. / под общ. ред. И.В. Ткаченко. Чебоксары: ООО «Издательский дом «Среда», 2022. С. 207–211.

4. Лазуткина Е.В. Некоторые вопросы теории элиты Вильфредо Парето и современность // Вестник КГПУ им. В.П. Астафьева. 2014. №2 (28). URL: https://cyberleninka.ru/article/n/nekotorye-voprosy-teorii-elity-vilfredo-pareto-i-sovremennost (дата обращения: 25.08.2025).

5. Медиаландшафт в 2023 году: аудитория, контент и генераторы повестки. URL: https://scan-interfax.ru/blog/medialandshaft-v-2023-godu-auditoriya-kontent-i-generatory-povestki/ (дата обращения: 25.08.2025).

6. Тоффлер Э. Третья волна. М.: ООО «Фирма «Издательство АСТ»», 2004, 672 с.

7. Труфанова Е.О. Информационное перенасыщение: ключевые проблемы // Философские проблемы информационных технологий и киберпространства. 2019. № 1(16). С. 4–21. DOI 10.17726/philIT.2019.1.16.1.

8. Digital Global Overview Report 2023. URL: https://wearesocial.com/wp-content/uploads/2023/03/Digital-2023-Global-Overview-Report.pdf (дата обращения: 25.08.2025).

9. Small G., Vorgan G. iBrain: Surviving the Technological Alteration of the Modern Mind. N.Y.: Harper Collis, 2009. 231 p.

УДК 347.7

О. В. Жевняк,
кандидат юридических наук, доцент,
Уральский федеральный университет
имени первого Президента России Б.Н. Ельцина

Постановка вопроса об экономическом понимании цифровых платформ для формирования общей части их правового режима

Аннотация. Формирование адекватного правового режима цифровых платформ невозможно без исследования их сущности. Цифровые платформы представляют собой многоаспектное явление, в котором можно выделить технико-технологический, экономический, политический, социальный и другие аспекты. Один из важнейших аспектов – экономический. Анализ экономической сущности цифровых платформ может присутствовать не только в специализированных экономических работах, но и в юридических исследованиях для понимания того, как должны регулироваться платформы, что необходимо учесть при формировании содержательной части правового регулирования. Цель работы – показать, какие вопросы следует проанализировать представителям юридической науки в сфере экономического понимания цифровых платформ для решения конечной прикладной задачи формирования общей части их правового режима. Решаются задачи выявления разных граней экономического понимания платформы и подходов к их анализу в трудах юристов на примере исследования одной из таких граней.

Ключевые слова: цифровые платформы, право цифровых платформ, теоретическая модель, экономическая сущность, многоаспектное явление, правовой режим, общая часть, платформенная экономика, экономика цифровых платформ, многосторонние рынки, двусторонние рынки

O. V. Zhevnyak,
Candidate of Law, Associate Professor,
Ural Federal University
named after the first President of Russia B.N. Yeltsin

Statement of the question of economic understanding of digital platforms for the formation of the general part of their legal regime

Abstract. The formation of an adequate legal regime for digital platforms is impossible without studying their essence. Digital platforms are a multi-faceted phenomenon, in which it is possible to distinguish technical and technological, economic, political, social and other aspects. One of the most important aspects is economic. Analysis of the economic essence of digital platforms can be present not only in specialized economic works, but also in legal studies to understand how platforms should be regulated, which must be taken into account when forming the substantive

part of legal regulation. The purpose of the work is to show what issues should be analyzed by representatives of legal science in the field of economic understanding of digital platforms to solve the final problem of forming the general part of their legal regime. The problems of identifying different facets of the economic understanding of the platform and approaches to their analysis in the works of lawyers are solved using the example of studying one of such facets.

Keywords: digital platforms, digital platform law, theoretical model, economic essence, multi-aspect phenomenon, legal regime, general part, platform economy, digital platform economy, multi-sided markets, two-sided markets

Введение. Формирование адекватного правового режима какого-либо явления невозможно без исследования его сущности. Цифровые платформы представляют собой многоаспектное явление, в котором можно выделить технико-технологический, экономический, политический, социальный и другие грани понимания. Одним из важнейших аспектов является экономический. При этом экономика представляет собой совокупность общественных отношений, складывающихся в процессе создания какого-либо продукта (ценности, блага) и его движения от производства до потребления (от производителя к потребителю), а продуктом могут быть как материальные, так и нематериальные блага. В таком широком понимании в сферу экономики следует включать не только отношения, связанные с производством и потреблением материальных благ, но и оказанием услуг, в том числе государственных и муниципальных, созданием и использованием результатов интеллектуальной деятельности и другие, включая отношения в сфере образования, культуры, искусства, здравоохранения, спорта, а также государственного управления. Цифровые платформы могут функционировать во всех указанных сферах.

Анализ экономической сущности цифровых платформ может присутствовать не только в специализированных экономических работах. Представляется, что межотраслевой характер исследования, привлечение специалистами одной области знаний других научных направлений может способствовать обогащению анализа, пониманию многоаспектности исследуемого явления, широкому взгляду на него. Полагаем, что представители юридической науки не только вправе анализировать сущность регулируемых явлений и отношений; можно рекомендовать им это делать для понимания того, как нужно регулировать отношения. Цифровые платформы, несомненно, обладают экономическими характеристиками, которые должны быть учтены при формировании содержательной части правового регулирования.

Обладание экономической сущностью следует из наблюдений даже обычного человека за практикой деятельности цифровых платформ, не говоря уже об ученом. По крайней мере, если исходить из принципа «чистоты юридического исследования», предполагающего, что ученый-правовед не обладает знаниями в других сферах, в том числе экономической, то на первых этапах юридического исследования, постановка вопроса о наличии экономической составляющей у платформ может быть гипотезой, подтверждение которой легко находится уже

после поверхностного ознакомления с трудами экономистов, посвященными цифровым платформам.

Цель настоящей работы – показать, какие вопросы следует проанализировать юридической науке в сфере экономического понимания цифровых платформ для решения конечной прикладной задачи формирования их правового режима.

Для достижения этой цели решаются задачи выявления разных граней экономического понимания платформы и подходов к их анализу в трудах юриста на примере исследования одной из таких граней.

В работе применяются феноменологический прием познания, анализ специальной литературы и обобщение.

Основная часть. Итак, цифровые платформы могут функционировать во всех экономических сферах, имея в виду широкий взгляд на понятие экономики, включая бизнес, государственное правление, сферы образования, культуры, искусства, здравоохранения, спорта. Правовой режим цифровых платформ может исходить из специфики разных видов платформ: маркетплейсов, поисковых систем, агрегаторов информации об услугах такси, отелей, платформ поиска работы, социальных сетей, мессенджеров и так далее.

Однако важным является обобщение и формирование общих правил, некой общей части права цифровых платформ. Другими словами, представляется, что право цифровых платформ должно включать не только особенную часть, учитывающую дифференциацию правил применительно к разным видам платформ, но и прежде всего, общую часть.

Поэтому юридическое исследование, направленное в итоге на формирование правового режима цифровых платформ, должно начаться с исследований сущности цифровой платформы как общего явления, выявления таких характеристик, которые подходят для описания любой платформы. Таким образом, нужно построить теоретическую модель цифровой платформы [1].

Учитывая многоаспектный характер цифровых платформ и признавая не только экономический подход к их пониманию, в данной работе мы сосредоточимся только на нем. Другим аспектам посвящены другие работы автора, например [2]. Поэтому говоря здесь только об исследовании экономической сущности платформ, мы должны показать, что задачей ученого-правоведа в этом направлении должно стать выявление экономических характеристик, которые подходят для описания платформ, независимо от области их применения.

Экономический взгляд на цифровые платформы, в свою очередь, тоже является многогранным. Выделим, как представляется, исходя из анализа литературы и феноменологического понимания явления цифровых платформ, основные подходы к выявлению их экономической сущности:

1) они могут рассматриваться как вид экономических общественных отношений, то есть некий особый экономический уклад. Представляется, что в данном аспекте можно признавать существование платформенной экономики – экономики, основанной на платформах;

2) микроэкономический взгляд на платформы позволяет рассматривать их как модель организации и управления деятельностью (бизнес-модель, органи-

зационно-управленческая модель). В этом проявляется организационно-управленческий аспект цифровых платформ;

3) цифровая платформа, по нашему мнению, выступает и как особый вид экономической деятельности;

4) ее можно рассматривать и в качестве хозяйствующего субъекта, участника экономических отношений, экономического агента;

5) цифровая платформа может рассматриваться как особый вид товара, относящийся к информационным товарам, что сближает платформу по своим характеристикам с другими информационными товарами, которые можно копировать, хранить, воспроизводить, а значит, и масштабировать без существенных затрат.

Указанные подходы к пониманию цифровой платформы как экономического феномена не являются исчерпывающими. Можно выявлять другие, более частные грани экономического платформенного феномена, например, рассматривать их как объект инвестирования, объект налогообложения. Особым экономическим взглядом на цифровую платформу может стать рассмотрение ее роли в государственном управлении (в связи с признанием государственного управления особым видом экономических отношений, в которых производится, доводится до потребителя и потребляется некий продукт государственной деятельности), что сопряжено с такой идеей, как «государство как платформа». Интересным предметом исследования является, на наш взгляд, рассмотрение цифровых платформ как инфраструктурного экономического феномена.

В качестве примера рассмотрим подходы к пониманию цифровых платформ как вида экономических отношений.

Этот аспект наиболее исследован применительно к рассмотрению платформ как вида рынка, другими словами, вида экономических рыночных отношений. Более того, представляется, что наибольшее количество экономических публикаций, посвященных цифровым платформам, исследует их именно с этой точки зрения. Популяризация платформ, введение в широкий оборот платформенной терминологии, по нашему мнению, произошло благодаря трудам зарубежных экономистов, анализирующих платформы как экономические отношения, а именно как двусторонние и многосторонние рынки. В этом аспекте сами платформы рассматриваются как модель организации рыночных отношений между участниками рынка. Другими словами, можно сказать, что сегодня экономические агенты для вовлечения в экономические отношения и продвижения своих продуктов выходят на платформенный рынок.

Стоит еще раз отметить, что через цифровые платформы могут быть организованы разные формы взаимодействия, прежде всего в рамках экономических отношений продавцов (исполнителей, правообладателей) и потребителей товаров (работ, услуг, результатов интеллектуальной деятельности). Поэтому рассмотрение данного экономического аспекта платформ должно осуществляться, учитывая прежде всего взаимодействие именно этих экономических агентов на платформенно организованном рынке. Однако не стоит забывать поставленную в рамках юридического исследования задачу выявления общих характеристик всех видов цифровых платформ.

Исследователи платформенной рыночной экономики описывают преимущественно производственные общественные отношения, которые складываются с участием хозяйствующих субъектов, осуществляющих предпринимательскую деятельность. Когда же речь идет, например, о государственном управлении, в котором активно развиваются платформенные отношения, или некоммерческих сферах функционирования платформ, не принято говорить об их принадлежности к рыночным отношениям. Однако основные выводы, сделанные по результатам рассмотрения платформенного рынка, могут быть применены, с учетом определенных ограничений, к иным сферам платформенных экономических отношений, прежде всего – к государственному управлению, а также другим нерыночным сферам функционирования платформ.

Во многих исследованиях отмечается центральная роль цифровых платформ в современных экономических отношениях. Так, в докладе Банка России для описания этих отношений используется термин «платформизация экономики», который показывает то, что платформы стали одним из наиболее значимых экономических явлений и играют все возрастающую роль в перераспределении ресурсов [6].

Д. Паркер, С. Чаудари и М. Ван Альстин, иллюстрируя то, насколько цифровые платформы «захватили» мир, проникли в разные сферы общественной жизни, вытесняя иные формы организации отношений, используют термин «революция платформ» [4].

А. Хассель и Ф. Зикер называют платформы «центральной чертой цифровой экономики и разрушительной силой в бизнес-ландшафте» [11].

В исследованиях цифровой экономики, проводимых международными организациями, отмечается, что ее основной особенностью является рост цифровых платформ, которые сосредоточены на данных и цифровом интеллекте [9. P. 45], что в такой экономике на создание стоимости более всего влияют две связанные между собой движущие силы: «платформизация и монетизация быстро растущего объема цифровых данных» [8. P. 25].

Ряд исследователей цифровых платформ, называя их новым принципом экономической организации, отмечают, что они меняют организацию конкуренции, работы и потребления и, таким образом, саму структуру современного общества [12]; они становятся доминирующими экономическими и социальными посредниками [13]. М. Кенни и Дж. Зисман сравнивают роль цифровых платформ как средства организации экономической деятельности в двадцать первом веке с той ролью, которую в конце девятнадцатого века играли корпорации. Эти авторы отмечают, что доминирующие цифровые платформы организуют и трансформируют пространство экономической деятельности, реорганизуют географию экономической активности [14. P. 64–73].

Появление и развитие платформ привело к существенным изменениям в экономической жизни в целом. В этом плане мы можем говорить о роли платформ в экономике, об их позитивном и негативном влиянии на экономические отношения. Есть основания говорить о том, что возникла новая экономика – экономика цифровых платформ. Ее следует рассматривать как следующий этап в продолжающихся изменениях, вызванных капитализмом и рыночной экономикой [13].

Некоторые авторы рассматривают экономику цифровых платформ как элемент шеринговой экономики, экономики совместного использования [5], так как она основана на новой форме взаимодействия производителей и потребителей, они зачастую совместно создают ценности, что в наибольшей степени проявляется на платформах совместного потребления. С этой точки зрения модели шеринговой экономики и платформенной экономики, скорее, могут пересекаться, однако в то же время занимают и свои собственные непересекающиеся ниши [15]. Всю платформенную экономику можно относить к экономике совместного использования только в широком смысле, с точки зрения совместного создания стоимости разными участниками платформенного рынка (например, продавцами, покупателями и владельцами платформ).

Платформенную экономику можно рассматривать как сетевую. Платформы создают сетевые отношения, в которых связи устанавливаются между участниками, но через платформу. По словам М. Кенни, Дж. Зисман и Д. Бирсон, «в этом смысле платформы больше похожи на традиционную коммутируемую сеть или коммутатор, а не на многоузловую структуру Интернета» [13]. К. Ван Гансен, К. Валайер и Д. Аллесси отмечают, что различные участники платформы «переплетаются» и формируют «сетевой рынок» [7. P. 18].

Представляется, что платформенная экономика обладает существенной спецификой по сравнению с традиционной рыночной экономикой, в связи с чем формируется новая экономическая теория – теория платформенной экономики. Большинство сложившихся методов экономического анализа не подходит для анализа онлайн-платформ, поэтому их использование может привести к неправильным рекомендациям по регулированию платформ.

Теория платформенной экономики и платформенных рынков начала разрабатываться с начала 2000-х годов; такие рынки назывались в ней «двусторонними рынками», «многосторонними рынками» или «многосторонними платформами». Как отмечает А. Гауэр, «экономисты рассматривают платформы как особые виды рынков, которые играют роль посредников обмена между различными типами потребителей, которые в противном случае не могли бы взаимодействовать друг с другом» [10. P. 1240]. М. Кенни и Дж. Зисман квалифицируют платформы как рынки в том смысле, что цифровые платформенные компании стали средой, в которой предприниматели открывают новые предприятия и управляют старыми [14. P. 58].

Рассмотрение платформ в качестве вида рынка, на котором особым образом взаимодействуют разные группы участников, является наиболее распространенным подходом к пониманию экономики платформ. При этом под рынком мы понимаем систему экономических отношений, возникающих между продавцами и покупателями в процессе обмена товарами, услугами и другими ресурсами. Это механизм, который позволяет согласовывать интересы участников: кто что хочет купить или продать, в каком объеме и по какой цене. Сущность рынка заключается в добровольности сделок и конкуренции между участниками. Рынок выполняет следующие функции: посредническую, функцию ценообразования, регулирующую, стимулирующую и информацион-

ную [3]. Платформенный рынок осуществляет все эти функции с присущими ему особенностями.

Рынки могут относиться к разным категориям, которые можно использовать и для описания платформенных рынков. Так, например, рынки бывают открытые и закрытые. Платформы чаще являются рынками, открытыми для вступления новых игроков – производителей товаров и услуг и их потребителей. Однако степень открытости может быть разная, по большому счету, она зависит от усмотрения владельца платформы. Выделяют организованные и неорганизованные рынки, регулируемые и нерегулируемые. Платформы, несомненно, являются организованными регулируемыми рынками. При этом владельцы платформ организуют рынок, предоставляя доступ к нему с помощью своей технико-технологической инфраструктуры, устанавливают правила взаимодействия сторон рынка и контролируют это взаимодействие.

В правовом исследовании при формировании теоретической модели цифровой платформы, включающей ее экономический аспект, необходимо проанализировать особенности рыночных и иных экономических отношений платформ. Среди них, например, можно выделить особенность состава участников отношений (участников рынка), рассмотреть наличие сетевых эффектов в таких отношениях и их особенности, проанализировать вытекающие из наличия сетевых эффектов характеристики отношений, включающие практику привязки к платформе, специфику ценообразования и другие, выявить того субъекта, который получает наибольшую выгоду в этих отношениях, рассмотреть особенности конкуренции и труда на платформенных рынках.

Все выявленные характеристики, обобщенно и укрупненно, без включения второстепенных элементов, должны быть положены в основу теоретической модели цифровой платформы, включающей ее экономический аспект. При этом в модель платформы в правовом исследовании должны включаться лишь те характеристики, которые имеют юридическое значение.

Эта модель должна быть дополнена характеристиками других граней экономического понимания цифровых платформ, изложенных выше. Затем теоретическая модель экономического понимания становится частью общей теоретической модели цифровой платформы, включающей ее другие аспекты (технико-технологический, политический, социальный и другие).

Заключение. Для юридических исследований, имеющих задачу формирование общего правового режима цифровых платформ, важно разобраться в их многоаспектной сущности и сформировать на этой основе теоретическую модель цифровой платформы, включающую основные общие характеристики платформ, имеющие юридическое значение.

Одним из центральных (наряду с технико-технологическим) взглядом на платформу является ее экономическая сущность. С этой точки зрения платформы могут рассматриваться как вид экономических общественных отношений, модель организации и управления деятельностью, вид экономической деятельности, в качестве хозяйствующего субъекта, как особый вид товара и др.

Так, например, платформу как вид экономических отношений следует рассматривать в качестве вида рыночных отношений, если мы говорим о сфере

бизнеса, однако выводы, сделанные по результатам анализа рыночной сущности платформ, вполне применимы, с учетом определенных ограничений, и к другим сферам деятельности, то есть ко всем экономическим отношениям, основанным на цифровых платформах. Для этого необходимо выявить признаки платформ как вида экономических отношений, которые послужат основой для формирования содержательной части их правового регулирования.

Подобным образом подлежат анализу другие грани экономической сущности платформ.

Построенная по результатам этих аналитических исследований теоретическая модель цифровой платформы, включающая ее экономический аспект, призвана стать частью общей теоретической модели цифровой платформы, включающей ее другие аспекты (технико-технологический, политический, социальный и другие).

Список литературы

1. Жевняк О. В. О теоретическом моделировании цифровой платформы как многоаспектного явления // Имущественные отношения в Российской Федерации. 2024. № 9 (276). С. 80–90. DOI: 10.24412/2072-4098-2024-9276-80-90.

2. Жевняк О. В. Цифровая платформа как технико-технологический феномен и его правовое значение // Вестник Пермского университета. Юридические науки. 2024. Вып. 4 (66). С. 541–561. DOI: 10.17072/1995-4190-2024-66-541-561.

3. Солдатенкова И. Что такое рынок? 2021 // Банки.ру. URL: https://www.banki.ru/wikibank/chto_takoe_ryinok/ (дата обращения: 08.09.2025).

4. Паркер Д., Альстин М., Чаудари С. Революция платформ: как сетевые рынки меняют экономику – и как заставить их работать на вас; перевод с английского Е. Пономаревой. Москва: Манн, Иванов и Фербер, 2017. 302 с.

5. Шилоносова Н. В., Бутрина Ю. В. Анализ развития онлайн-платформ в условиях шеринговой экономики // Вестник Южно-Уральского государственного университета. Серия: Экономика и менеджмент. 2019. Т. 13, № 4. С. 167–179. DOI: 10.14529/em190417.

6. Экосистемы: подходы к регулированию: Доклад для общественных консультаций. Банк России. Апрель 2021 года. URL: https://cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021.pdf (дата обращения: 08.09.2025).

7. Digital Platform for public services: Final Report ISA2 action 2016.10: ELISE: European Location Interoperability Solutions for eGovernment / K. Van Gansen, C. Valayer, D. Allessie. European Union, 2018. 119 p. URL: https://interoperable-europe.ec.europa.eu/sites/default/files/document/2018-10/330043300REPJRCDigitalPlatformsBM-D2.5FinalReportv051018.pdf (дата обращения: 08.09.2025).

8. Digital Economy Report 2019. Value Creation and Capture: Implications For Developing Countries. United Nations Conference on Trade and Development.

United Nations. Geneva, 2019. 194 p. URL: https://unctad.org/system/files/official-document/der2019_en.pdf (дата обращения: 08.09.2025).

9. Digital Economy Report. Pacific Edition. 2021. Towards Value Creation and Inclusiveness. United Nations Conference on Trade and Development. United Nations. Geneva, 2023. 113 p. URL: https://unctad.org/publication/digital-economy-report-2021 (дата обращения: 08.09.2025).

10. Gawer A. Bridging differing perspectives on technological platforms: Toward an integrative framework // Research Policy. 2014. Vol. 43, Iss. 7. Pp. 1239–1249. DOI: 10.1016/j.respol.2014.03.006.

11. Hassel A., Sieker F. Contested Terrain: three battlefields in which to study the digital economy. Background Paper For “Work In The Digital Age: The Challenge Of Platform Firms”. BRIE Working Paper, February 2021. URL: https://brie.berkeley.edu/sites/default/files/contested_terrain_22022021_final.pdf (дата обращения: 08.09.2025).

12. Kenney M., Rouvinen P., Zysman J. Employment, Work, and Value Creation in the Era of Digital Platforms. 2019 // Digital Work and the Platform Economy. DOI: 10.4324/9780429467929-2.

13. Kenney M., Zysman J., Bearson D. What Polanyi Teaches Us: The Platform Economy and Structural Change // SSRN Electronic Journal. 2020. DOI: 10.2139/ssrn.3678967.

14. Kenney M., Zysman J. The platform economy: restructuring the space of capitalist accumulation // Cambridge Journal of Regions. Economy and Society. 2020. № 13. P. 55–76. DOI: 10.1093/cjres/rsaa001.

15. Sharing economy – General principles. International standard ISO 42500:2021 (E). URL: https:/standards.iteh.ai/catalog/standards/sist/caac27bf-7c99-4163-ae1e e07d173b43b3/iso-42500-2021 (дата обращения: 08.09.2025).

УДК 347.1

А. В. Олейникова,
кандидат юридических наук, доцент,
Донецкий государственный университет,
А. В. Бакуров,
магистрант,
Донецкий государственный университет

Особенности регулирования деятельности агрегаторов отечественным законодательством

Аннотация. В статье отражены современные тенденции, реализуемые законодателем в вопросах регулирования деятельности цифровых платформ и владельцев агрегаторов информации. Федеральный закон от 01.04.2025 №-41-ФЗ наделяет их полномочиями оператора по сбору персональных данных, проведению процедур идентификации и аутентификации. Это поможет обеспечить прозрачность и реализацию принципа добросовестности между участниками гражданских правоотношений в цифровом пространстве.

Ключевые слова: владелец агрегатора информации, биометрические персональные данные, добросовестность пользователей маркетплейсов

A. V. Oleynikova,
Candidate of Law, Senior Lecturer,
Donetsk State University,
A. V. Bakurov,
Master's student,
Donetsk State University

The features of aggregators' activities regulation by domestic legislation

Abstract. The aim of the article is to investigate the current trends implemented by the legislator in the regulation of the digital platforms and owners of information aggregators activities. The Federal Law No-41-FL of 01.04.2025 gives them the powers of an operator to collect personal data, conduct identification and authentication procedures. This will help ensure transparency and the implementation of the principle of good faith between participants in civil legal relations in the digital space

Keywords: owner of the information aggregator, biometric personal data, integrity of marketplace users

Введение. Формирование цифровых рынков – одна из главных тенденций развития экономики на современном этапе. Ключевую роль в этом играют агрегаторы товаров и услуг. Причем, среди различных видов их деятельности – оказание услуг, информирование, инвестирование, продажа товаров – именно последний делает их организаторами товарооборота [4. С. 77]. Это, так называе-

мые, маркетплейсы или торговые агрегаторы. Считают, что они «формируют новые индустрии» [6. С. 76]. Среди них присутствуют крупные компании, чья ежемесячная аудитория составляет десятки миллионов человек [17. С. 3]. Причем это не только отечественные (Яндекс.Маркет, Ozon и Wildberries, Avito), но и ряд зарубежных (AliExpress, Booking.com, Apple Store, Google Play и др.). Их относят к цифровым платформам, доминирующим на рынке [17. С. 10]. Однако, несмотря на значимость, законодательное определение таких понятий как «маркетплейс» или «торговый агрегатор» отсутствует. Поскольку эти понятия родовые с нормированным определением агрегатора, вероятно, законодатель считает это достаточным.

Основная часть. Так всеобъемлющее описание, включавшее большинство характеристик агрегатора, было дано Федеральным законом от 29 июля 2018 г. № 250-ФЗ [8]. Законодатель, нормируя правовой статус владельца агрегатора, изначально вменял ему оказание услуг преимущественно информационного характера. Позже Федеральный закон от 31 июля 2020 г. № 290-ФЗ «О внесении изменений в Закон Российской Федерации «О защите прав потребителей», по сути, наделил полномочиями торгового агрегатора, расширив возможность безналичных расчетов по договорам, заключенным между потребителями и продавцами, расчетами наличными средствами через сайт владельца агрегатора.

Таким образом, начиная с 2020 г. владелец агрегатора был наделен обязательством к участию в наличных расчетах с покупателем, что максимально сблизило с маркетплейсами. Однако, ряд цивилистов считает, что легальное определение торговых агрегаторов (маркетплейсов) все же необходимо [5. С. 19; 6. С. 75]. Т. Ф.Тимофеева и В. В. Тимофеев описали основные особенности торговых агрегаторов, которые делают их привлекательными для пользователей и способствуют их дальнейшему активному продвижению на рынке [6. С. 75]. Например, это удобная для взаимодействия информационно-технологическая среда; прозрачность и возможность зарегистрироваться новым субъектам для взаимовыгодных отношений; снижение издержек. Это способствует популяризации цифровых рынков, росту числа пользователей.

Исходя из особенностей регулирования деятельности цифровых платформ, понимаем, что законодатель избрал универсальный подход, пойдя по пути распространения имеющихся норм на новые субъекты, лишь точечно дополняя их регулирование адресными нормами.

В настоящее время правовое регулирование цифровых платформ основано на нормах Конституции, Гражданского и Налогового кодексов Российской Федерации, а также ряда федеральных законов [6. С. 73; 15. С. 63].

Однако это не полный перечень нормативных правовых актов, регламентирующих деятельность владельцев агрегаторов. Так, в виде частного нормотворчества разрабатываются механизмы саморегулирования. В развитии цифровых платформ четко наметилась тенденция к их укрупнению и поглощению доминирующими цифровыми платформами, что подпадает под действие антимонопольного законодательства [17. С. 9]. Однако имеющаяся тенденция к формированию, так называемых, «экосистем», расценивается Минэкономразвития как

положительная [17. С. 4]. Вместе с Центральным Банком разрабатываются способы их регулирования (опубликованы «Концепция регулирования цифровых платформ и экосистем», Доклад Банка России «Экосистемы: подходы к регулированию») [17. С. 3, 10, 16].

В целом отметим, что регулирование гражданско-правовых отношений, реализуемых в цифровом пространстве посредством Интернета – пожалуй, самая молодая и бурно развивающаяся отрасль права.

В рамках статьи рассмотрим, как регулируется между пользователями цифровых платформ один из основополагающих принципов договорного права – принцип добросовестности гражданских правоотношений и свободы договора (ст. 1, 10 Гражданского Кодекса Российской Федерации) [2, 3]. Он реализуется за счет выстраивания «прозрачных» отношений между сторонами договора, при их полной открытости, предоставлении достоверной информации (запрашиваемых персональных данных, сертификатов, деклараций соответствия и т. п.) (согласно ч. 2.1 ст. 9, ст. 41 Закона РФ «О защите прав потребителей») [12; 5. С. 21]. При невыполнении этих обязательств предусмотрены санкции [6. С. 77]. В свою очередь, покупатель осуществляет свою деятельность через личный кабинет на сайте агрегатора, содержащий его персональных данные, что также нормируется [7; 15. С. 64]. Причем регулирование идентификации пользователей цифровых платформ было существенно реформировано Федеральным законом от 29 декабря 2022 г. № 527-ФЗ (ред. от 28.12.2024) «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации» [9].

Можно отметить, что упомянутый выше Закон является ключевым для формирующегося сейчас в российском законодательстве института «биометрических персональных данных» (БПД). По сути, это новейшее направление в развитии отечественного гражданского права. Проведем анализ НПА, регламентирующих деятельность владельцев агрегаторов в вопросах идентификации (аутентификации) физлиц. При этом, по мнению Хандрыга Д. О. до подписания Федерального закона от 29.12.2022 № 527-ФЗ нормирование БПД характеризовалось разрозненностью и отсутствием системного подхода. Не были детально регламентирован функции Единой биометрической системы (ЕБС), что создавало пространство для возможных злоупотреблений в отношении субъектов БПД [16. С. 197]. Отметим, что изначально понятие биометрических персональных данных было легитимировано ст. 11 Федерального закона от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», внесшего соответствующие дополнения в Федеральный закон от 27 июля 2006 года № 152-ФЗ, описавшего данные биометрии как позволяющие устанавливать личность человека (субъекта персональных данных) по данным его биологических особенностей [11]. Причем, согласно не подвергавшейся редакции статье 12 Федеральный закон № 152-ФЗ в настоящее время попрежнему может осуществляться трансграничная передача персональных данных, в том числе БПД на территории иностранных государств, являющихся

сторонами Конвенции Совета Европы, т. е. проводящими уже более десятилетия в отношении России политику ужесточения санкций.

Согласно Федеральному закону от 1 апреля 2025 г. № 41-ФЗ «О создании государственной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации», регуляция деятельности агрегаторов непосредственно подпадает под НПА, легитимирующие сбор БПД [14]. Так, данный закон вносит изменения в Федеральный закон от 7 февраля 1992 г. № 2300-I «О защите прав потребителей», наделяя владельцев агрегатора правом предоставить возможность прохождения аутентификации пользователям (продавцам и потребителям) с использованием ЕБС в соответствии со ст. 10 ФЗ от 29 декабря 2022 г. № 527-ФЗ. Он также обязывает владельцев агрегатора проводить идентификацию с использованием федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – единая система идентификации и аутентификации, ГИС ЕСИА).

Уточним, что понятие ГИС ЕСИА также было нормировано совсем недавно. Так, Федеральный закон от 28 декабря 2024 г. N 521-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» в статье 6 внес соответствующие изменения в абз.2 ч.1 ст. 155.2 Гражданского процессуального кодекса Российской Федерации с использованием биометрических персональных данных [3, 13].

Таким образом, новейшие изменения в законодательстве призваны реализовать принципы добросовестности гражданских правоотношений и свободы договора, обеспечив идентификацию его сторон.

Однако не следует игнорировать риски, возникающие при этом. Так, начатое в России создание многочисленных Единых Реестров (индивидуальных предпринимателей, юридических лиц, ЕСИА и т. п.), а также деятельность платформы Госуслуги реализуется с использованием технологии распределенного реестра. При этом передача материала в информационно-телекоммуникационной сети Интернет идет через облачные хранилища зарубежных провайдеров, через центры обработки данных, расположенные на территории их государств. Это многократно увеличивает вероятность хищения информации.

Предоставление услуг на основе облачных технологий характеризуется возросшим количеством уязвимостей и внешних угроз, что обусловлено использованием открытых каналов связи, а сбои при предоставлении сервисов и разглашение информации могут нанести значительный экономический ущерб [1].

Учитывая, что более 11 лет в отношении России ведется санкционная недружественная политика большинством европейских государств, а также США и Великобританией, противоречащая ряду международных норм, то не выглядит достаточной степень защиты трансграничной передачи данных предписываемая согласно п. 3 ст. 12 Федерального закона «О защите персональных дан-

ных» о том, что «оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных» [10, 11]. Исходя из новых обязательств владельцев агрегаторов перед пользователями и государством, предписываемых законодательством, назрела необходимость более жесткой регламентации трансграничной передачи персональных данных, тем более БПД.

Еще одной особенностью нормотворчества в вопросах законодательного регулирования деятельности агрегаторов, которую удалось установить при написании данной статьи, является активное участие самих субъектов цифрового права в обсуждении и редакции новых законопроектов. Так, в частности, в первом чтении Проект ФЗ № 41-ФЗ № 842276-8 1.1 в п. 1.4 ст. 3 содержал императивную норму, предписывавшую владельцам агрегаторов обязательство проводить всем участникам аутентификацию через ЕБС. По результатам письма Федерального общества сетевой торговли (ФОСТ) главе правительства, норма теперь носит рекомендательный характер.

Как уже было отмечено выше цифровые платформы обязаны обеспечить возможность такой идентификации при желании продавца и размещать информацию об этом, чтобы ее видели покупатели.

Действительно, научно-технический прогресс и цифровизация не должны затрагивать, а тем более ущемлять права и законные интересы физических лиц, тем более в вопросах сбора БПД [16, С. 198]. Возможное участие агрегаторов в формировании ЕБС помогает обнаружить имеющуюся проблему и делает актуальным пересмотр норм, регулирующих трансграничную передачу персональных данных. В частности, действие ст. 12 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» должно быть пересмотрено.

Заключение. Следовательно, в настоящее время в стране реализуется законодательное регулирование гражданских правоотношений, осуществляемых посредством цифровой среды. Работа цифровых платформ и владельцев агрегаторов в области защиты прав потребителей теперь будет тесно сопряжена с деятельностью, создаваемой Государственной информационной системой противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий. Это поможет обеспечить прозрачность и реализацию принципа добросовестности между участниками гражданских правоотношений в цифровом пространстве.

Список литературы

1. Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: автореф. дис. … канд. юрид. наук. Казань. 2017. 31 с.

2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202007040001 (дата обращения: 15.07.2025).

3. Гражданский процессуальный кодекс Российской Федерации // Собрание законодательства Российской Федерации. 2002. № 46. ст. 4532 // СПС «ГАРАНТ». URL: Гражданский процессуальный кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ (ГПК ... | Система ГАРАНТ) (дата обращения 18.08.2025).

4.Крусс И. А. Нормативно-правовое регулирование цифровой торговой инфраструктуры в Российской Федерации // Вестник Тверского государственного университета. Серия Право. 2023. №. 4. С. 75–82.

5.Колесниченко О.В., Панкратова Д.В. Реализация товаров через маркетплейсы: проблемы осуществления и защиты прав потребителей// Национальная безопасность. 2024. № 3. С. 17№27. DOI: 10.7256/2454-0668.2024.3.71092.

6. Тимофеева Т. Ф., Тимофеев В. В. Проблемы правового регулирования торгового агрегатора как разновидности цифровой технологической платформы // Oeconomia et Jus. 2022. № 3. С. 73-79. DOI: https://doi.org/10.47026/2499-9636-2022-3-73-79.

7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Российская газета. 2006. № 165.

8. Федеральный закон «О внесении изменений в Закон Российской Федерации "О защите прав потребителей"» от 29 июля 2018 г. № 250-ФЗ. // СПС «Консультант плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_303537 (дата обращения: 18.08.2025).

9. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «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» // СЗ РФ. 2023. № 1 (ч. 1). Ст. 19.

10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Российская газета. 2006. 29 июля. № 165.

11. Федеральный закон от 25 июля 2011 г. N 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Российская газета. 2011. № 162.

12. Федеральный закон от 7 февраля 1992 г. № 2300-1- ФЗ «О защите прав потребителей» (ред. от 11.06.2021 г.) // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_305

13. Федеральный закон от 28 декабря 2024 г. № 521-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета. 9 января 2025 г. № 1-2.

14. Федеральный закон от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2025. № 14. Ст. 1574 2025. URL: https://sozd.duma.gov.ru/bill/842276-8 (дата обращения: 02.08.2025).

15. Фликов И.И., Савоськин А.В. Ответственность владельца агрегатора и продавца перед потребителем по договору купли-продажи на маркетплейсе // Территория новых возможностей. Вестник Владивостокского государственного университета. 2023. Т. 15. № 3 С. 60–71. DOI: https://doi.org/10.24866/VVSU/2949-1258/2023-3/060-071

16. Хандрыга Д. О. Правовое регулирование биометрических персональных данных в Российской Федерации // Вестник Российской правовой академии. 2024. № 1. С. 191–201. DOI: https://doi.org/10.33874/2072-9936-2024-0-1-191-201

17. Шелепов А. В., Колмар О.И. Регулирование цифровых платформ в России // Вестник международных организаций. 2024. Т. 19, № 2. С. 110–126.

УДК 004.738.5:351.78

Р. В. Торшин,
доцент,
НИУ «Высшая школа экономики»

Разработка цифрового маркетплейса комплексной безопасности с использованием low-code технологий

Аннотация. В статье представлен опыт создания инновационного цифрового маркетплейса комплексной безопасности с использованием low-code платформы Lovable.dev. Исследование раскрывает особенности применения современных веб-технологий для решения проблемы фрагментарности рынка услуг информационной безопасности в России. Проанализированы преимущества и недостатки low-code подхода при создании специализированных B2B-платформ в сфере безопасности. Рассмотрены перспективы развития маркетплейс-модели для объединения экспертов по различным направлениям комплексной безопасности бизнеса.

Ключевые слова: цифровой маркетплейс, информационная безопасность, low-code технологии, комплексная безопасность, веб-разработка, цифровая трансформация, B2B-платформа

R.V. Torshin,
S.Associate Professor,
HSE University

Development of a digital comprehensive security marketplace using low-code technologies

Abstract. The article presents the experience of creating an innovative digital comprehensive security marketplace using the Lovable.dev low-code platform. The study reveals the features of using modern web technologies to solve the problem of fragmentation of the information security services market in Russia. The advantages and disadvantages of the low-code approach when creating specialized B2B platforms in the field of security are analyzed. The prospects for the development of a marketplace model for uniting experts in various areas of comprehensive business security are considered.

Keywords: digital marketplace, information security, low-code technologies, comprehensive security, web development, digital transformation, B2B platform

Введение. Российский рынок информационной безопасности демонстрирует устойчивый рост на уровне 23–30 % ежегодно, достигнув объема 299–339 млрд рублей в 2024 году [1]. Несмотря на положительную динамику, сохраняется проблема фрагментарности услуг в сфере комплексной безопасности, что создает высокие транзакционные издержки для бизнеса. 75 % российских

компаний сталкиваются с киберугрозами, однако вынуждены обращаться к десяткам различных поставщиков для получения услуг по кибербезопасности, физической охране, правовой защите и другим направлениям безопасности [2].

Цель исследования – анализ возможностей создания единого цифрового маркетплейса комплексной безопасности с использованием современных low-code технологий для решения проблемы фрагментарности рынка услуг информационной безопасности.

Основная часть.

Методология и технологическое решение. Для реализации проекта была выбрана low-code платформа Lovable.dev, позволяющая создавать сложные веб-приложения с минимальным объемом программирования. Выбор технологического стека обусловлен необходимостью быстрого создания и итерации прототипа в условиях динамично развивающегося рынка.

Сравнительный анализ подходов к разработке представлен в табл. 1.

Таблица 1

Сравнительный анализ подходов разработки

Критерий	Low-Code	Традиционная разработка	No-Code
Время создания MVP	Недели	Месяцы	Дни-недели
Стоимость	$1-5K	$20-50K	$100-1K
Гибкость кастомизации	Средняя	Очень высокая	Низкая
Скорость изменений	Высокая	Средняя	Очень высокая
Контроль над кодом	Ограниченный	Полный	Отсутствует

Архитектура и функционал маркетплейса безопасности (MVP по ссылке https://secure-biz-landing.lovable.app) [3].

Разработанная платформа объединяет экспертов по 20 направлениям комплексной безопасности бизнеса, включая:

1. Цифровая безопасность: кибербезопасность, защита персональных данных, антивирусная защита.

2. Физическая безопасность: охранные системы, контроль доступа, видеонаблюдение.

3. Бизнес-безопасность: кадровая безопасность, антикоррупционное сопровождение, защита от мошенничества.

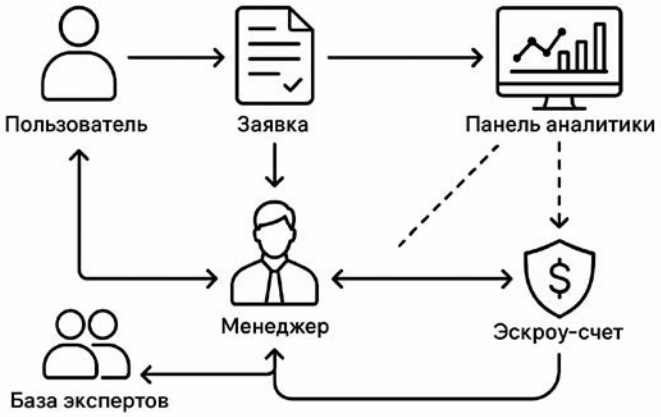
Бизнес-модель платформы основана на следующем алгоритме:

1. Клиент размещает заявку с описанием задачи.

2. Менеджер платформы подбирает квалифицированного эксперта.

3. Средства резервируются на счете до выполнения работ.

4. Эксперт получает оплату через 7 дней после завершения проекта.



Архитектура цифрового маркетплейса комплексной безопасности

Результаты и анализ эффективности. Применение low-code подхода позволило сократить время разработки MVP с 6 месяцев до 3 недель при снижении затрат в 10 раз по сравнению с традиционной разработкой. Платформа обеспечивает адаптивный дизайн для всех устройств, интегрированную систему управления контентом и базовые инструменты аналитики.

Однако выявлены критические ограничения:

– сложность верификации компетенций экспертов;

– ограниченные возможности глубокой кастомизации интерфейса;

– зависимость от внешней платформы разработки;

– проблемы масштабирования при росте числа пользователей.

Перспективы развития и рекомендации. Анализ показал, что успех маркетплейса безопасности на 80 % зависит от качества экспертной базы, а не от технологического совершенства платформы. Рекомендуется поэтапное развитие проекта:

Фаза 1 (0–6 месяцев): создание системы верификации экспертов и привлечение 50-100 квалифицированных специалистов;

Фаза 2 (6–18 месяцев): разработка мобильного приложения и интеграция с CRM/ERP системами;

Фаза 3 (18+ месяцев): региональная экспансия и развитие корпоративного B2B сегмента.

Прогнозируемая модель монетизации включает комиссию 10–15 % с экспертов, премиум-подписки (5000₽/мес) и корпоративные тарифы (от 50 000 ₽/мес).

Заключение. Исследование подтвердило эффективность low-code технологий для быстрого создания и тестирования инновационных бизнес-решений в сфере информационной безопасности. Разработанный маркетплейс комплексной безопасности решает актуальную проблему фрагментарности рынка услуг ИБ в России.

При условии решения выявленных проблем с верификацией экспертов и качеством услуг, проект имеет потенциал захвата 1–2 % рынка услуг ИБ для

МСБ с прогнозируемой выручкой 150–350 млн рублей к 2030 году. Опыт разработки демонстрирует возможности современных веб-технологий для цифровой трансформации традиционных отраслей экономики.

Список литературы

1. Аналитический обзор российского рынка информационной безопасности // TAdviser. 2024. URL: https://www.tadviser.ru/index.php/Статья:Рынок_ИБ_России (дата обращения: 10.09.2025).
2. Отчет о состоянии информационной безопасности в России 2024 / Центр мониторинга и реагирования на компьютерные атаки. М.: ЦМРКА, 2024. С. 15–28.
3. MVP маркетплейса безопасности. URL: https://secure-biz-landing.lovable.app (дата обращения: 10.09.2025).
4. Васильев А. И., Петров С. М. Цифровые платформы в сфере информационной безопасности: тенденции и перспективы // Вопросы кибербезопасности. 2023. № 4 (56). С. 23–31.
5. Иванова Е. Н. Low-code разработка как инструмент цифровой трансформации бизнеса // Информационные технологии в экономике. 2024. № 2 (38). С. 45–52.
6. Сидоров П. К., Федорова Л. В. Маркетплейс-модели в B2B-сегменте: анализ эффективности // Российский журнал менеджмента. 2023. Т. 21, № 3. С. 67–84.
7. Третьяков Д. А. Проблемы верификации экспертов на цифровых платформах // Управление персоналом и интеллектуальными ресурсами в России. 2024. № 1 (64). С. 18–25.
8. Чернов В. С., Белова А. П. Анализ драйверов роста российского рынка информационной безопасности // Экономический анализ: теория и практика. 2024. № 7 (538). С. 1287–1305.
9. Brown J., Smith R. Low-code platforms adoption in enterprise environments: A comprehensive analysis // Journal of Business Technology. 2024. Vol. 15, № 3. P. 45–62. URL: https://jbtech.example.org/vol15/iss3/45 (дата обращения: 10.09.2025).
10. Davis M., Wilson K. Marketplace platforms in B2B security services: challenges and opportunities // International Journal of Information Security. 2023. Vol. 22, № 4. P. 891–908. URL: https://link.springer.com/article/10.1007/s10207-023-00525-6 (дата обращения: 10.09.2025).

УДК 347.78

А. С. Васильева,
аспирант,
Санкт-Петербургский государственный
экономический университет

Классификация видов искусственного интеллекта в контексте права интеллектуальной собственности

Аннотация. Данная статья имеет своей целью формирование научного представления о классификации видов искусственного интеллекта в контексте права интеллектуальной собственности. Большое внимание уделено рассмотрению классификаций, в основе которых лежат такие критерии как функциональные возможности искусственного интеллекта, конкретные технологии реализации искусственного интеллекта, области применения. Предложена классификация видов искусственного интеллекта в зависимости от получаемого результата в соотношении с результатами интеллектуальной деятельности человека и классификация технологии в зависимости от получаемого результата при генерации искусственным интеллектом. Сформулировано определение генеративного искусственного интеллекта.

Ключевые слова: искусственный интеллект, классификация, вид, правосубъектность, автономность, функциональные возможности, сильный и слабый искусственный интеллект

A. S. Vasileva,
postgraduate student,
St. Petersburg State University of Economics

Classification of types of artificial intelligence in the context of intellectual property law

Abstract. This article aims to form a scientific understanding of the classification of types of artificial intelligence in the context of intellectual property law. Much attention is paid to the consideration of classifications based on such criteria as the functional capabilities of artificial intelligence, specific technologies for the implementation of artificial intelligence, and areas of application. A classification of types of artificial intelligence is proposed depending on the result obtained in relation to the results of human intellectual activity. A classification of technology is also proposed

depending on the result obtained when generating artificial intelligence. A definition of generative artificial intelligence is formulated.

Keywords: artificial intelligence, classification, type, legal capacity, autonomy, functionality, strong and weak artificial intelligence

Классификация видов искусственного интеллекта (далее – ИИ) имеет важное значение для определения функциональных возможностей ИИ, позволяет учитывать степень автономности ИИ, дает представление об областях применения ИИ. В этой связи необходимо привести слова С. С. Алексеева, который отмечал, что «подлинно научные классификации имеют значение не только для систематизации изучаемых явлений. Они в то же время служат ступенью к изучению содержания явлений, нередко способствуют правильному уяснению их функций и природы. Правда, это во многом зависит от того, какой из признаков изучаемых явлений (сущность или внешний, формальный) положен в основу классификации» [1. С. 467]. Поэтому для определения правового положения ИИ и правового режима его результатов необходимо учитывать вид ИИ. Так, П. М. Морхат указывает, что правосубъектность юнита ИИ должна быть своего рода «плавающей» в зависимости от типа юнита ИИ, от его изначальной экспектативной или текущей реальной функционально-целевой нагрузки [10. С. 31]. Что именно автор понимает под типом юнита ИИ не указывается, при этом, следуя из анализа выделенных исследователем типов ИИ, можно сказать, что речь идет именно о видах ИИ. По нашему представлению, с приведенным высказыванием П. М. Морхата трудно не согласиться, поэтому необходимо рассмотреть виды ИИ для того, чтобы определить, чем являются результаты, созданные с применением ИИ, и каково правовое положение уже самого ИИ.

Однако, прежде чем перейти к классификации значимой в контексте права интеллектуальной собственности, остановимся на классификациях, которые существуют в законодательстве и в доктрине. Это необходимо для того, чтобы разобраться в природе самого ИИ и его возможностях.

В Европейском союзе ИИ классифицируется в зависимости от степени риска при использовании ИИ на недопустимый (ИИ, который несет явную угрозу безопасности, направлен на социальную оценку), высокий (ИИ, применяемый на транспорте, в роботизированной хирургии, для оценивания экзаменов, для сортировки резюме при приеме на работу, для биометрической идентификации), ограниченный (при взаимодействии с данным ИИ необходимо уведомление пользователя, например, если текст создан с помощью ИИ и опубликован с целью информирования по вопросам, представляющим общественный интерес, то такой текст должен быть помечен, как созданный ИИ) и минимальный (видеоигры с поддержкой ИИ или фильтры спама) [19].

В науке классифицируют данную новую технологию на ИИ, основанный на правилах, и ИИ, основанный на обучении. Первый работает с использованием, как уже видно из названия, предопределенных правил и логики. Решения принимаются на основе четких инструкций, представленных экспертами-людьми. ИИ, основанный на обучении, может адаптироваться и совершенствоваться с течением времени, но требует больших объемов данных. Данный вид

использует алгоритмы для выделения закономерностей и принятия решений. ИИ в этом случае гибкий, поэтому может улучшаться с течением времени по мере обработки большого количества данных [21].

Другой классификацией ИИ по функциональным возможностям является деление на реактивный ИИ, ИИ с ограниченной памятью, социальный и самосознающий ИИ. Реактивный ИИ не основывает принятие своих решений на предыдущем опыте. Примером такого вида является Deep Blue – шахматная компьютерная программа. Deep Blue игнорирует все, на основании чего ранее принималось решение, кроме шахматных правил, т. е. запрета на повторение одного и того же хода три раза. Второй вид – ограниченная память ИИ, на данный вид памяти можно ссылаться при принятии будущих решений. Обучение ИИ осуществляется в данном случае на фактах и событиях, имевших место в прошлом. Примерами такого вида являются беспилотные автомобили, принятие решений которыми осуществляется на прошлом опыте. Они принимают решение на основе разметки полос движения, расположении светофоров, изгиба дороги, скорости движения других автомобилей, что требует определенного времени отслеживания. Третий вид – социальный ИИ. Данный вид ИИ не существует. Он предполагает, что в будущем ИИ будет способен оценивать эмоциональное состояние других агентов или сущностей. Этот вид оценивает поведение других на основе представления о том, что у них есть собственные мысли и эмоции, влияющие на их поведение. Последний вид – самосознающий ИИ. Данный вид будет формировать представление о самом себе. Однако это станет возможно только, когда будет изучен человеческий интеллект [24]. Прогрессивность этой классификации очевидна, она включает два вида ИИ – социальный и самосознающий, которые будут максимально приближены к человеку и его возможностям.

Иной классификацией является деление видов ИИ по конкретным технологиям реализации ИИ и по областям применения. Во-первых, обработка естественного языка. Эта технология позволяет машинам взаимодействовать с людьми естественным образом, в режиме разговора. Обработка естественного языка используется в различных приложениях: от чат-ботов и голосовых помощников до сервисов перевода. Например, Siri, Google Assistant используют обработку естественного языка для понимания голосовых команд и реагирования на них. Во-вторых, компьютерное зрение, которое позволяет машинам интерпретировать и осмысливать визуальные данные, такие как изображения и видео. Компьютерное зрение применяется для распознавания лиц, для медицинской визуализации в целях обнаружения опухолей на рентгеновских снимках. В-третьих, робототехника. В данном случае роботы на основе ИИ способны выполнять физические задачи автономно или полуавтономно. Например, робототехника широко применяется в производстве, где роботы выполняют такие задачи, как сборка, сварка и упаковка. В здравоохранении роботы помогают при проведении хирургических операций и реабилитации [27].

И. А. Филипова отмечает, что в специальной литературе по информатике нередко перечисляются следующие разновидности ИИ: автоматизированный ИИ (выполняет рутинные задачи); вспомогательный (оптимизирует решения,

выполняемые человеком); расширенный (способен осуществлять поддержку человеческого мышления в нестандартных ситуациях); автономный (осуществляет деятельность самостоятельно, подобно человеку) [17. С. 22-23].

Далее предлагается рассмотреть классификации видов ИИ, значимые для права интеллектуальной собственности и определения того, чем является результат, созданный с использованием ИИ, – результатом интеллектуальной деятельности (далее – РИД) (ИИ в данном случае является инструментом в руках человека-творца) или результатом деятельности ИИ (результат, сгенерированный ИИ автономно, который внешне не отличается от РИД человека и обладает уникальностью (признак, характеризующий результат деятельности ИИ, обладающий отличительными характеристиками от других результатов деятельности ИИ, сгенерированных при идентичном промте и наборе данных)).

В зависимости от функциональных возможностей ИИ классифицируется на такие виды, как слабый и сильный (общий). Последний будет способен решать любые интеллектуальные задачи любой сложности [5]. Сильный ИИ будет автономно решать различные задачи [12]. Представляется, что его результаты будут результатами деятельности ИИ, а сам ИИ будет автором в случае внесения изменений в законодательство. Об этом также указывают зарубежные исследователи [22]. Слабый ИИ используется для выполнения определенной задачи [2. С. 54–55]. Его результаты являются РИД, так как ИИ выступает в качестве инструмента. Эти два вида описываются в российском стратегическом документе [12]. Как отмечает В. П. Константинов, разработка сильного ИИ произведет научную революцию, в связи с чем необходимо заранее подготовить почву для его будущего внедрения, если это внедрение будет необходимо [9. С. 147]. При этом некоторые исследователи указывают, что российские официальные акты отражают больше функциональные возможности сильного ИИ [3. С. 52]. В рамках данной классификации также выделяют сверхсильный ИИ (сверх-ИИ, супер-ИИ), возможности которого будут превосходить способности человека, а сам ИИ будет обладать самосознанием [20]. Однако пока этот вид ИИ находится в рамках научной фантастики. Отмечается, что искусственный сверхинтеллект будет изобретен в будущем в рамках квантовых вычислений [23]. Так как на сегодняшний день не существует ни сильного ИИ, ни сверх-ИИ, то разграничивать данные виды достаточно сложно. Эти слова подтверждает тот факт, что некоторые авторы отождествляют два ранее упомянутых вида [14]. При этом лауреат Нобелевской премии по химии, генеральный директор Google DeepMind Демис Хассабис отметил, что с вероятностью 50 % будет достигнут уровень общего (сильного) ИИ к 2030 году [4].

Теперь следует рассмотреть классификацию видов ИИ в зависимости от получаемого результата в соотношении с РИД:

– ИИ, создающий (генерирующий) результаты, сопоставимые с объектами авторских и смежных прав. Например, YandexART 2.5 может сгенерировать изображения с текстом и выбрать подходящий под конкретную задачу стиль [28];

– ИИ, создающий (генерирующий) результаты, сопоставимые с объектами патентных прав. Например, всемирно известные случаи генерации ИИ DABUS патентоспособных результатов;

– ИИ, создающий (генерирующий) результаты, сопоставимые со средствами индивидуализации. Например, на сайте GENLOGO возможно сгенерировать изображение, которое может стать средством индивидуализации, исходя из названия, слогана или краткого описания, а также категории (авто, мебель и другие) [16]. Отечественная разработка от Студии Артемия Лебедева также может сгенерировать графические материалы на основании данных, внесенных пользователем. Права на сгенерированные результаты предоставляются пользователю на условиях исключительной лицензии на весь срок охраны исключительного права и на территории использования всего мира с момента отображения их в аккаунте пользователя [11].

При этом такие результаты могут быть как РИД, так и результатами деятельности ИИ. В данном случае важно подчеркнуть, какую роль играл ИИ, была ли творческая корректировка его деятельности человеком.

Другой классификацией является деление видов на основе зависимости ИИ от человека на автономный и подчиненный. Автономный ИИ будет способен к самообучению, к своей воле, к своим целям [7]. Подчиненный ИИ, следуя из названия, подчинен чьей-либо воле. Следовательно, только результаты автономного ИИ будут результатами деятельности ИИ.

В науке также представлена классификация ИИ по творческому потенциалу:

– слабое влияние на финальный результата (текстовые редакторы для исправления ошибок, стилистики). ИИ почти не проявляет свой творческий потенциал;

– влияние на финальный результат, но использование в качестве инструмента (по идее автора-человека) (ИИ проявляет творческий потенциал, но не в полной мере. Свобода творчества ограничена контекстом или небольшим количеством данных для анализа и обучения);

– финальный результат непредсказуем (творческий потенциал ИИ проявляется в полной мере) [6].

Классификацию видов ИИ можно произвести в зависимости от получаемого результата при генерации ИИ:

– уникальный ИИ. Результат его деятельности будет неочевиден для его разработчиков, пользователей. Результат будет сопоставим с объектами интеллектуальных прав. При этом ИИ будет выступать в качестве автора результата при автономной работе. Такой результат будет результатом деятельности ИИ;

– копирующий ИИ. В данном случае невозможно предсказать, какой будет результат, но он точно будет схож с загруженным набором данных. ИИ в этом случае ничего уникального не создает. Он лишь компилирует известные данные в определенный результат. Как отмечает Д. А. Казанцев, результат ИИ собирается, компилируется, обрабатывается синтетически, содержательно никогда [8]. Примером «работы» копирующего ИИ является иск газетных компаний The Yomiuri Shimbun, The Yomiuri Shimbun, Osaka и The Yomiuri Shimbun, Seibu

(входят в состав The Yomiuri Shimbun Holdings) к Perplexity AI, Inc, который был подан в Токийский окружной суд. Истцы требуют прекратить использование статей и возмещение ущерба в размере 2,17 млрд иен. В своем иске The Yomiuri Shimbun утверждает, что Perplexity копировала статьи из цифрового сервиса Yomiuri Shimbun Online (YOL) и отправляла своим пользователям ответы с контентом, похожим на эти статьи. Отмечается, что ответчик без разрешения использовал большое количество статей и изображений The Yomiuri Shimbun для поисковой системы на основе генеративного ИИ. The Yomiuri Shimbun утверждает, что это нарушало право на воспроизведение и право на публичное распространение в соответствии с Законом об авторском праве [29];

– корректирующий ИИ. Корректировка может быть грамматической, логической, орфографической, стилистической. На основании ранее рассмотренной классификации влияние ИИ на финальный результат будет слабым. Результат будет РИД человека. Корректирующий ИИ по своим функциональным возможностям является разновидностью слабого ИИ.

ИИ также можно классифицировать по классу задач, которые он решает, на аналитико-вычислительный и аналитико-генеративный. Первый тип направлен на решение отдельных прикладных задач (обработка естественного языка текста и речи; компьютерное зрение и др.). Второй тип ИИ также решает задачу, определенную для него разработчиком (функциональная предопределенность), лежащие в его основе алгоритмы опираются на вероятностные модели, что в итоге ведет к получению заранее достоверно непрогнозируемых результатов [18].

Еще одной классификацией является деление видов ИИ в зависимости от назначения. Выделяют предиктивный ИИ, который используется для прогнозирования будущих результатов, в частности, для прогнозирования спроса и оценки риска; вспомогательный ИИ направлен на повышение производительности и эффективности; разговорный ИИ обеспечивает взаимодействие, подобное человеческому. В эту классификацию также включен генеративный ИИ [26]. При этом генеративный ИИ является не видом, а типом ИИ. И. А. Филипова отмечает, что «в этом случае вид – это понятие, характеризующее систему искусственного интеллекта по внешним признакам (демонстрируемому уровню решения интеллектуальных задач), а тип показывает каким образом данная система принимает решение». Автором выделены такие типы, как 1) модерационный (основан на технологии модерации контента за счет анализа данных. Например, модерационный ИИ используются для выявления и удаления нежелательного контента); 2) предиктивный (проводит анализ и выстраивает прогноз с помощью накопленных и доступных данных, осуществляя предиктивную (предсказательную) аналитику. Например, позволяет предусмотреть последствия принимаемых решений в государственном управлении); 3) генеративный [17. С. 26]. Традиционно под генеративным ИИ понимают тип ИИ, который на основе больших наборов данных генерирует новые результаты (включая текст, изображения, аудио или видео) в ответ на запрос, который может быть сформулирован пользователем без применения навыков программирования [15]. Е. А. Обухова определяет генеративный ИИ как комплекс технологических решений, позволяю-

щий создавать новый оригинальный контент, а также самостоятельно обучаться на большом массиве данных [13]. Зарубежные исследователи дают такое определение генеративному ИИ как ИИ, способный создавать оригинальный контент, такой как текст, изображения, видео, аудио или программный код, в ответ на промт или запрос пользователя [25]. Соглашаясь с авторами, что генеративный ИИ способен создавать определенный результат, стоит отметить, что данный результат не следует называть новым или оригинальным, необходимо выработать иной критерий. Новизна и оригинальность являются категориями патентного права, стремление наделить такими характеристиками результаты генеративного ИИ, сопоставимые с объектами авторских прав, представляется, неверным. Под генеративным ИИ предлагается понимать, следуя тем характеристикам, которые были выделены нами ранее, тип ИИ, который автономно генерирует (создает) уникальные результаты в ответ на запрос пользователя. Такое толкование генеративного ИИ несколько сужает рассмотренные ранее подходы определения данного понятия, однако представленная дефиниция позволяет отделить обычный ИИ, которым пользуются в качестве инструмента для создания РИД, и генеративный ИИ, который автономно генерирует (создает) результат.

Подводя итог, можно сказать, что при определении правового положения ИИ и правового режима его результатов необходимо учитывать вид ИИ. В работе были рассмотрены классификации видов ИИ, представленные в отечественной и зарубежной доктрине. Предложены две классификации видов ИИ в зависимости от получаемого результата в соотношении с РИД и в зависимости от получаемого результата при генерации ИИ.

Список литературы

1. Алексеев С. С. Собрание сочинений. В 10 т. [+ Справоч. том]. Том 1: Гражданское право: Сочинения 1958–1970 годов. М.: Статут, 2010. 495 с.
2. Баюк Д. А., Попова А. В. Правовые и этические проблемы искусственного интеллекта: учебник для магистратуры. М.: Прометей, 2022. 300 с.
3. Ватьян А. С., Гусарова Н. Ф., Добренко Н. В. Системы искусственного интеллекта: учебное пособие. СПб: Университет ИТМО, 2022. 186 с.
4. Глава Google DeepMind: у AGI 50% шанс появиться к 2030 году // Хабр. URL: https://habr.com/ru/news/930670/ (дата обращения: 20.08.2025).
5. Городнова Н. В. Моделирование развития и внедрения систем «слабого» и «сильного» искусственного интеллекта: социально-экономические аспекты // Вопросы инновационной экономики. 2022. № 1. С. 123–140. doi: 10.18334/vinec. 12.1.113717
6. Гурова М. Е. Право интеллектуальной собственности: авторское право на труды искусственного интеллекта // Скиф. Вопросы студенческой науки. 2021. № 6 (58). С. 231–234.
7. Жданов А. Автономный и подчиненный искусственный интеллект. 31 мая 2015 г. // ПостНаука. URL: https://postnauka.org/video/47828 (дата обращения: 06.04.2025).

8. Запись научного подкаста #65 РОБОТ НАПИСАЛ СИМФОНИЮ. КАК ЗАЩИТИТЬ АВТОРСКИЕ ПРАВА? // Journal of Digital Technologies and Law [Электронный ресурс]. URL: https://t.me/JournalDTL/2048 (дата обращения: 14.04.2025).

9. Константинов П. В. Влияние информационных технологий на принципы гражданского процесса (сравнительно-правовое исследование на примере России и Франции): дис. … канд. юрид. наук: 5.1.3; УрГЮУ им. В.Ф. Яковлева. Екатеринбург, 2022. 351 с.

10. Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дис. … докт. юрид. наук: 12.00.03; РГАИС. Москва, 2018. 420 с.

11. Иронов Н. Уникальный бренд за секунды – логотип и айдентика с нейросетью Студии Артемия Лебедева. Оферта // ironov.artlebedev.ru [Электронный ресурс]. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/ https://ironov.artlebedev.ru/static/offer-ru.pdf (дата обращения: 15.07.2025).

12. О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента Российской Федерации от 10 октября 2019 г. № 490: офиц. текст по состоянию на 15 февраля 2024 г. // Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.

13. Обухова Е. А. Генеративный искусственный интеллект как драйвер развития высокотехнологических секторов экономики России // Экономика и управление инновациями. 2024. №3 (30). С. 70-78.

14. Пшегорская Ю. В. К вопросу о понятии искусственный интеллект: неопределенность терминов // Гуманитарные аспекты повседневности: проблемы и перспективы в XXI веке: сборник научных трудов. Воронеж: Автономная некоммерческая организация по оказанию издательских и полиграфических услуг "НАУКА-ЮНИПРЕСС", 2025. С. 97-105.

15. Самарцева М. В. Правовой режим результатов, создаваемых генеративным искусственным интеллектом // Цифровое право. 2024. № 5 (3). С. 19-65. https://doi.org/10.38044/2686-9136-2024-5-3-5

16. Создайте логотип онлайн в 5 кликов! ИИ, фирменный стиль и брендбук // GENLOGO [Электронный ресурс]. URL: https://genlogo.com/ (дата обращения: 15.07.2025).

17. Филипова И. А. Правовое регулирование искусственного интеллекта: учебное пособие, 3-е изд., обновл. и доп. Нижний Новгород: Нижегородский госуниверситет, 2025. 321 с.

18. Чурилова А. А., Трынченкова Н. А. Охраноспособность результатов, созданных с помощью искусственного интеллекта // Интеллектуальные права в цифровую эпоху: избранные аспекты: коллективная монография. Вып. 19. / рук. и науч. ред. д. ю. н. М. А. Рожкова; вступ. ст.: В. А. Корнеев. М.: ГАУГН Пресс, 2023. 438 с. С. 140-152. DOI 10.18254/S6049894-5-6

19. AI act // European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (дата обращения: 06.04.2025).

20. Eliacik E. Isn`t AI already super? Artificial super intelligence is on the way. July 12, 2022 // Dataconomy. URL: https://dataconomy.com/2022/07/12/what-is-artificial-super-intelligence/ (дата обращения:15.01.2024).

21. Federico Schiano di Pepe. + 7 Types of AI: Understanding Artificial Intelligence in 2025 // teachfloor. URL: https://www.teachfloor.com/blog/types-of-ai#types-of-ai-rule-based-vs-learning-based-ai (дата обращения: 06.08.2025).

22. Grimmelmann J. There's No Such Thing as a Computer-Authored Work – And It's a Good Thing, Too // Columbia Journal of Law & the Arts. 2016. № 39. P. 403-416.

23. Hanif Khan. (2021). Types of AI | Different Types of Artificial Intelligence Systems // ResearchGate. URL: https://www.researchgate.net/publication/355021812_Types_of_AI_Different_Types_of_Artificial_Intelligence_Systems_fossgurucomtypes-of-ai-different-types-of-artificial-intelligence-systems (дата обращения: 08.08.2025).

24. Hintze A. From Reactive Robots to Sentient Machines: The 4 types of AI. November 14, 2016 // Livescience. URL: https://www.livescience.com/56858-4-types-artificial-intelligence.html (дата обращения: 07.08.2025).

25. Stryker C., Scapicchio M. What is generative AI? // IBM. URL: https://ww.ibm.com/think/topics/generative-ai#Use+cases+for+generative+AI (дата обращения: 10.08.2025).

26. The Ultimate Breakdown of Different AI Types and Models // GoSearch. URL: https://www.gosearch.ai/blog/breakdown-of-different-ai-types-and-models/ (дата обращения: 08.08.2025).

27. Understanding the Varied Types of Artificial Intelligence and Their Impact // CertLibrary Blog. URL: https://www.certlibrary.com/blog/understanding-the-varied-types-of-artificial-intelligence-and-their-impact/ (дата обращения: 12.08.2025).

28. YandexART 2.5 // Яндекс. URL: https://ya.ru/ai/art (дата обращения: 15.07.2025).

29. Yomiuri Sues U.S. AI Startup over Use of Articles; Perplexity Allegedly Used Over 100,000 News Stories // The Japan News by THE YOMIURI SHIMBUN. URL: https://japannews.yomiuri.co.jp/society/crime-courts/20250810-274484/ (дата обращения: 01.09.2025).

УДК 347.78

С. Ф. Грищук-Бучка,
доктор права, адвокат, патентный поверенный,
преподаватель Международного независимого университета,
Молдова

Правовой режим компьютерной программы в Республике Молдова: эволюция и современные вызовы

Аннотация. Статья посвящена исследованию правового режима компьютерных программ в Республике Молдова в контексте цифровой трансформации. Целью работы является анализ эволюции нормативного регулирования, выявление современных вызовов и оценка соответствия национального законодательства международным стандартам. Рассматриваются положения Закона № 230/2022, особенности охраны программ как объектов авторского права, специфика договорных отношений, включая трудовые и подрядные договоры, а также механизмы защиты прав в цифровой среде. Акцент сделан на необходимости правовой определенности и развития правоприменительной практики.

Ключевые слова: право, цифровые технологии, компьютерные программы, авторское право, интеллектуальная собственность, программное обеспечение, договор, AGEPI, исключительное право

S. F. Grișciuc-Bucica
Doctor of Law, Attorney-at-Law, Patent Attorney,
Lecturer at the Free International University of Moldova

Legal regime of computer programs in the Republic of Moldova: evolution and contemporary challenges

Abstract. The article explores the legal regime of computer programs in the Republic of Moldova within the context of digital transformation. The objective of the study is to analyze the evolution of normative regulation, identify current challenges, and assess the alignment of national legislation with international standards. The paper examines the provisions of Law No. 230/2022, the specific features of protection of software as objects of copyright, the contractual framework–including employment and service contracts–as well as mechanisms for the enforcement of rights in the digital environment. Particular attention is given to the need for legal certainty and the development of consistent law enforcement practices.

Keywords: law, digital technologies, computer programs, copyright, intellectual property, software, contract, AGEPI, exclusive right

Современное информационное общество переживает этап глубокой цифровой трансформации, в ходе которой ключевую роль играют объекты интеллектуальной собственности и соответствующие права на них как нематери-

альные активы, обладающие значительным экономическим потенциалом. Во многом именно они становятся основой экономических, управленческих и социальных процессов. В этом контексте особое значение приобретают компьютерные программы, которые, несмотря на относительную «молодость» как правовая категория, являются одним из наиболее динамично развивающихся, практически значимых и экономически эффективных объектов интеллектуальной собственности.

В рамках национальной правовой системы Республики Молдова правовой режим компьютерных программ прошел последовательную эволюцию. Если ранее он регулировался положениями Закона № 139 от 2 июля 2010 года [2], то с 9 декабря 2022 года вступил в силу новый Закон № 230 от 28 июля 2022 года «Об авторском праве и смежных правах» [1], который отменил предшествующий акт и утвердил обновленные подходы к охране объектов авторского права в условиях цифровой экономики.

История развития правового регулирования компьютерных программ в Республике Молдова может быть условно разделена на несколько этапов.

Первое системное регулирование авторского права на территории Республики Молдова было закреплено в Законе № 293-XIII от 23 ноября 1994 года «Об авторском праве и смежных правах» [3]. Этот акт содержал положения, заимствованные из советской правовой традиции, но адаптированные к новым рыночным реалиям. В нем отсутствовало четкое определение правового режима компьютерных программ, вследствие чего возникали сложности при квалификации таких объектов в рамках договоров и судебных дел.

Закон № 139 от 2 июля 2010 года стал значительным шагом вперед: он впервые системно включил положения о правовой охране компьютерных программ, определил их как объекты авторского права, эквивалентные литературным произведениям, и расширил перечень охраняемых действий [2]. Особое внимание было уделено электронной форме воспроизведения, а также регулированию лицензирования, в том числе в цифровой среде.

Однако технологические и цифровые изменения привели к необходимости более глубокой адаптации законодательства. Закон № 139/2010 был признан утратившим силу в связи с принятием нового Закона № 230 от 28 июля 2022 года [1]. Новый закон учитывает реалии цифровой трансформации, административную практику AGEPI, а также сложившуюся судебную практику последних лет, ориентируясь на повышение правовой определенности и усиление механизмов защиты прав.

Компьютерная программа как объект авторского права. В соответствии со статьей 23 Закона Республики Молдова № 230 от 28 июля 2022 года «Об авторском праве и смежных правах» [1, ст. 23], компьютерные программы прямо отнесены к объектам авторского права и охраняются аналогично литературным произведениям. Данный подход соответствует положениям международных соглашений (в частности, ст. 23 Договора ВОИС по авторскому праву [5] , статьи 10 ТРИПС [6] и статьи 1 Директивы 2009/24/ЕС [7]), устанавливающих универсальные стандарты охраны программного обеспечения в качестве произведения.

Согласно статье 3 указанного Закона, правовая охрана на компьютерную программу распространяется:

– на исходный код программы;

– объектный код (машиночитаемое представление);

– подготовительные материалы, полученные в процессе разработки, при условии, что они могут быть использованы для последующего создания программы (например, спецификации, алгоритмические схемы, схемы проектирования), а также руководства. Идеи, приемы, способы функционирования, математические концепции и принципы, лежащие в основе любого элемента компьютерной программы, включая те, которые лежат в основе ее интерфейсов, алгоритмы и языки программирования не подлежат охране [1].

Ключевым критерием охраноспособности, в соответствии со статьей 23 Закона, выступает оригинальность формы выражения *в том смысле, что представляет собой собственное интеллектуальное творение автора. Для определения того, пользуется ли она правом на охрану, не применяются никакие другие критерии* [1]. Правовая охрана никоим образом не распространяется на идеи, методы, математические концепции, принципы функционирования или алгоритмы, лежащие в основе программы. Соотвественно, охраняется именно форма выражения, независимо от функциональной ценности самой программы.

Авторское право на компьютерную программу возникает с момента создания произведения и не требует обязательной регистрации. Однако, согласно действующему авторскому праву, регистрация в AGEPI (Агентстве по интеллектуальной собственности Республики Молдова) [4], может быть осуществлена добровольно. Она имеет важное правовое значение в целях удостоверения даты создания, авторства и доказательства при судебных спорах или коммерческом использовании. Соответственно **регистрация в AGEPI не порождает права**, а лишь подтверждает факт создания – это принцип охраны ex lege ТРИПС, [6]. Процедура регистрации включает представление исходного и/или объектного кода, аннотации, а также информации об авторе. Несмотря на то, что правовая охрана возникает в силу факта создания, регистрация служит средством фиксации прав и выступает презумпцией авторства, пока не доказано иное.

Особенность компьютерных программ как объектов авторского права заключается в их техническом характере: в отличие от традиционных литературных произведений, эстетическая или художественная ценность не является критерием охраны. Как отмечается в правовой доктрине (Samuelson P., Nimmer R.), ценность программы определяется ее функциональностью («поведением»), а не литературными достоинствами исходного кода [8].

Кроме того, действующее законодательство Республики Молдова в данном вопросе гармонизировано с правовыми системами других стран региона. Например, законодательство Румынии, Украины, Беларуси и Российской Федерации также предусматривает охрану компьютерных программ как самостоятельных объектов авторского права, признавая их оригинальность и прикладную ценность. При этом уточняются составные части программ, включая подготовительные материалы и документацию, сопровождающую программный продукт.

Таким образом, включение компьютерных программ в сферу авторского права отражает эволюцию правового регулирования интеллектуальных продуктов и адаптацию законодательства Республики Молдова к реалиям цифровой экономики и международным стандартам.

Закон Республики Молдова № 230/2022 закрепляет дифференцированный подход к правам автора на компьютерную программу, подразделяя их на личные неимущественные и имущественные. Такой подход соответствует устоявшимся доктринальным позициям в области авторского права и международным обязательствам, принятым Республикой Молдова.

Согласно статье 11 указанного Закона [1], к числу моральных (личных неимущественных) прав автора относятся:

– право на признание авторства – обеспечение юридического признания лица автором созданной программы, включая запрет на присвоение авторства другими лицами;

– право на имя – возможность требовать указания имени автора при использовании произведения или отказаться от такого указания (право на анонимность или псевдоним);

– право на соблюдение целостности произведения – право на защиту произведения от искажений, извращений, изменений или иных действий, способных нанести ущерб чести, достоинству и деловой репутации автора;

– право на раскрытие произведения – право решать, будет ли произведение обнародовано, каким образом и когда.

Эти права являются неотчуждаемыми, непередаваемыми и бессрочными, они сохраняются за автором даже в случае полной передачи имущественных прав третьим лицам [1].

В Законе Республики Молдова № 230/2022 исключительные права автора компьютерной программы получили специализированное нормативное закрепление в ст. 25, отличающееся от общего режима, предусмотренного ст. 12 [1].

Это подчеркивает техническую специфику программного обеспечения как объекта авторского права, что также соответствует практике Европейского союза и положениям Директивы 2009/24/ЕС.

Во-первых, охрана распространяется даже на **временные формы воспроизведения,** необходимые для функционирования программы (загрузка, запуск, сохранение), что приближает регулирование к современным моделям использования ПО, включая SaaS и облачные сервисы. Во-вторых, прямо урегулированы вопросы **адаптации и преобразования**, при этом автор адаптации сохраняет права на производный результат. В-третьих, закреплен **отдельный режим проката**, отличающийся от продажи: исчерпание права распространяется только на первую продажу, а **право на сдачу** в прокат (внаем) **сохраняется** за правообладателем. Таким образом, ст. 25 представляет собой специализированный режим правовой охраны, который учитывает особенности оборота программных продуктов в условиях цифровой экономики и охватывает широкий спектр практических ситуаций, связанных с воспроизведением, распространением и модификацией программного обеспечения.

Исключительные права автора компьютерной программы могут быть отчуждены или предоставлены в пользование на основании гражданско-правового договора, в том числе договора отчуждения исключительных прав или лицензионного соглашения. Законодатель подчеркивает необходимость наличия: письменной формы сделки, определения предмета передачи (программа или ее компоненты), указания срока, территории, способа использования, а также вознаграждения [1. С. 29–30].

Допускается как полная передача исключительного права, так и предоставление неисключительной лицензии – в зависимости от воли сторон и условий соглашения. Важно отметить, что даже при передаче исключительных имущественных прав, автор сохраняет свои личные неимущественные права, а также право на вознаграждение, если иное не установлено договором. Это позволяет обеспечить баланс между интересами автора и лиц, инвестирующих в разработку или использование программного обеспечения.

Таким образом, система прав автора компьютерной программы, закрепленная в Законе № 230/2022, отражает современные подходы к охране интеллектуальной собственности и учитывает как юридическую, так и коммерческую специфику программного обеспечения как объекта авторского права.

Договорное регулирование в сфере программного обеспечения. Заключение договоров, касающихся создания, передачи и использования компьютерных программ, занимает центральное место в практике оборота прав интеллектуальной собственности. Закон № 230/2022 устанавливает как общие, так и специальные положения, регулирующие договорные отношения между авторами, работодателями, заказчиками и пользователями программного обеспечения. [1]. Согласно положениям Закона, исключительные имущественные права автора могут быть переданы по договору полностью или частично, на определенный срок или без ограничения срока. Передача прав оформляется в письменной форме, с четким указанием объема, территории, срока и вознаграждения.

Лицензионные соглашения (ст. 32) допускают как исключительную, так и неисключительную лицензию. Условия использования программы, способы, сроки и территория действия лицензии должны быть определены в договоре. Безвозмездная лицензия допустима только при прямом указании в соглашении. Таким образом, эффективность договорной конструкции определяется точностью формулировок, соблюдением письменной формы и ясным распределением прав и обязанностей сторон [1].

Трудовые и подрядные отношения: авторство и исключительное право. Особое внимание в Законе Республики Молдова № 230 от 28 июля 2022 года «Об авторском праве и смежных правах» уделяется вопросам правового режима компьютерных программ, созданных в рамках трудовых или гражданско-правовых отношений. Такие программы, как правило, создаются в рамках исполнения должностных обязанностей, технических заданий или на основании заключенного договора, что требует ясного правового урегулирования прав на результат.

Согласно ст. 14 Закона № 230/2022, если программа создана работником в рамках выполнения служебных обязанностей или конкретного задания рабо-

тодателя, исключительные имущественные права на нее принадлежат работодателю, если иное не предусмотрено договором. Это положение закрепляет презумпцию служебного авторства, при которой работодатель приобретает права на использование и распоряжение программой, включая передачу и лицензирование.

При этом за работником сохраняются личные неимущественные права, в том числе право на признание авторства, на имя и на защиту от искажения произведения. Закон также предусматривает возможность выплаты автору дополнительного вознаграждения, если такая норма включена в трудовой договор, коллективное соглашение или локальный нормативный акт (внутренний регламент предприятия, положение о премировании и др.) [1]. В случаях, когда разработка программы осуществляется не в рамках трудового договора, а на основании гражданско-правового контракта (договор подряда, договор оказания услуг, договор на разработку программного обеспечения и т. п.), правовой режим и распределение исключительных прав должны быть прямо урегулированы в договоре. В противном случае, при отсутствии соответствующих положений, исключительное право остается за автором-исполнителем, что может повлечь юридическую неопределенность и потенциальные споры.

С учетом этого важным условием при заключении как трудовых, так и подрядных договоров является юридическая фиксация правового статуса создаваемой программы, а также распределение прав и обязанностей сторон по отношению к результату интеллектуальной деятельности. Рекомендуется детализировать: объем передаваемых прав (исключительные или неисключительные), территорию действия, сроки и способы использования, условия вознаграждения.

Отсутствие таких условий, как показывает практика, приводит к коллизиям между работодателем, заказчиком и разработчиком, особенно в случае коммерциализации программного продукта или передачи его третьим лицам.

Защита авторских прав на компьютерные программы. В целях обеспечения эффективной охраны прав авторов и правообладателей на компьютерные программы закон № 230/2022 закрепляет широкий спектр юридических средств, направленных на пресечение нарушений и восстановление нарушенных прав.

Согласно главе IX Закона, автор или иное правообладающее лицо вправе требовать [1]:

– официального признания авторского права;

– прекращения противоправных действий, в том числе распространения незаконных копий;

– возмещения причиненного ущерба, включая упущенную выгоду;

– выплаты компенсации в размере от 500 до 500 000 леев за каждое нарушенное право;

– уничтожения контрафактных экземпляров программы и оборудования, использованного для их создания и тиражирования;

– публикации решения суда за счет нарушителя как меры репутационного воздействия и др.

Кроме того, в Законе предусмотрены административные и уголовные меры, применяемые в случаях систематических или особо значительных нарушений. К числу таких мер относятся:

– блокировка доступа к сайтам, распространяющим нелегальный контент;

– удаление программ с хостингов, маркетплейсов и других платформ;

– привлечение нарушителей к ответственности в порядке КоАП или Уголовного кодекса Республики Молдова.

Отдельную роль в механизме охраны прав играет Агентство по интеллектуальной собственности (AGEPI), осуществляющее [4]:

– добровольную регистрацию программ и фиксацию авторства;

– экспертную оценку в случае споров;

– консультативное сопровождение субъектов авторского права при заключении договоров;

– правопросветительскую и методическую деятельность.

Эволюция правового регулирования компьютерных программ в Республике Молдова демонстрирует стремление национального законодателя обеспечить их комплексную и адекватную охрану как самостоятельных объектов интеллектуальной собственности в условиях цифровой экономики. Закон №230/2022 закрепил детализированные положения, касающиеся личных и имущественных прав авторов, механизмов их защиты, а также правовых условий передачи исключительных прав. Его принятие позволило гармонизировать национальное законодательство с международными стандартами и заложило основу для дальнейшего развития практики в данной сфере.

В то же время в процессе применения законодательства выявляются **актуальные вызовы**, обусловленные не отсутствием регулирования как такового, а необходимостью его надлежащего толкования и практического внедрения. К числу таких вызовов относятся:

– **определение авторства** в коллективных и служебных разработках при недостаточной договорной фиксации прав и обязанностей сторон;

– **реализация механизма компенсации**, в частности доказывание размера ущерба;

– **правоприменение в цифровой среде**, включая блокировку и удаление незаконного контента, что сопряжено с техническими и процедурными трудностями и требует межведомственного взаимодействия;

– **отсутствие единых методических подходов и типовых договоров**, что снижает предсказуемость регулирования отношений между авторами, работодателями и пользователями программного обеспечения;

– **необходимость развития судебной и административной практики**, обеспечивающей единообразное толкование норм Закона № 230/2022 и их адаптацию к новым цифровым реалиям.

Таким образом, дальнейшее развитие правовой охраны компьютерных программ в Республике Молдова зависит не только от качества и полноты законодательных норм, но и от формирования устойчивой правоприменительной практики, основанной на балансе интересов авторов, работодателей и пользователей программного обеспечения. Только при условии такой институциональ-

ной поддержки нормы Закона № 230/2022 будут функционировать эффективно и сбалансировано, обеспечивая интересы авторов-разработчиков, работодателей и пользователей программного обеспечения.

Список литературы

1. Об авторском праве и смежных правах: Закон Республики Молдова nr. 230 от 28.07.2022// Мониторул Официал ал Р. Молдова № 278-282 ст. 578 от 09.09.2022. URL: https://www.legis.md/cautare/getResults?doc_id=133204&lang=ru (дата обращения: 10.09.2025).
2. Об авторском праве и смежных правах: Закон Республики Молдова nr. 139 от 02.07.2010// Мониторул Официал ал Р. Молдова N 191-193 ст.630 от 01.10.2010. URL: https://weblex.md/item/view/id/c7e408c052e4023d0d5f303e22655390 (дата обращения: 11.09.2025).
3. Об авторском праве и смежных правах: Закон Республики Молдова nr. 293-XIII от 23.11.1994// Мониторул Официал ал Р.Молдова N 13 ст.124 от 02.03.1995, Переопубликован: Мониторул Официал N 18-19 ст.55 от 08.02.2003. URL: https://weblex.md/item/view/id/f7ce9f2085521a3f5ec3cfd64033bc44 (дата обращения: 10.09.2025).
4. Сайт Государственного агентство по интеллектуальной собственности Республики Молдова (AGEPI). URL: https://www.agepi.gov.md/ (дата обращения: 16.09.2025).
5. WIPO Copyright Treaty December 20, 1996. URL: https://www.wipo.int/wipolex/en/treaties/textdetails/12744 (дата обращения: 11.09.2025).
6. Agreement on trade-related aspects of intellectual property rights. URL: https://www.wto.org/english/docs_e/legal_e/27-trips.pdf (дата обращения: 12.09.2025).
7. Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. URL: https://www.wipo.int/wipolex/ru/legislation/details/8612 (дата обращения: 12.09.2025).
8. Samuelson P., *F*unctionality and Expression in Computer Programs: Refining the Tests for Software Copyright Infringement, 2015. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667740 (дата обращения: 14.09.2025).

УДК 347.77:004.8

А. В. Закомолдин,
кандидат юридических наук, доцент,
Центр бизнес-образования Торгово-промышленной палаты
г. Тольятти

Проблемы защиты прав на объекты интеллектуальной собственности, созданные с помощью ИИ

Аннотация. Перспективы, возникшие в современных условиях развития технологий искусственного интеллекта (ИИ), ставят ряд вопросов, требующих не только вдумчивых ответов, но и обоснованных решений, в том числе на законодательном уровне. С развитием и популяризацией генеративных нейросетей, позволяющих создавать тексты, изображения и видеоролики, проблематика права интеллектуальной собственности перешла на качественно иной уровень: ключевой вопрос, который начал беспокоить пользователей данных систем, касается определения автора произведения, созданного с помощью нейросетевых технологий и возможности защиты прав на данное произведение. Отсутствие четкой конкретики по данному вопросу актуализирует исследования в указанном направлении, в целях формирования научно-обоснованных позиций и интеграции таковых в действующее правовое регулирование.

Ключевые слова: авторское право, право интеллектуальной собственности, цифровые технологии, большие языковые модели, искусственный интеллект, нейросети, объекты интеллектуальной собственности, защита прав авторов, современные технологии в праве

A. V. Zakomoldin,
Candidate of Law, Associate Professor,
Center of Business Education of Chamber of Commerce and Industry of Togliatti

Problems of intellectual property rights protection created with AI

Abstract. The prospects that have emerged in modern conditions of the development of artificial intelligence (AI) technologies pose a number of questions that require not only thoughtful answers, but also informed decisions, including the legislative level. With the development and popularization of generative neural networks that allows to create texts, images and videos, the issue of intellectual property law has moved to a qualitatively different level: the key issue that began to bother users of these systems concerns the identification of the author of the work created with neural network technologies and the possibility of protecting the rights to this work. The lack of clear specifics on this issue actualizes research in this direction, in order to form scientifically sound positions and integrate them into the current legal regulation.

Keywords: copyright, intellectual property law, digital technologies, large language models, artificial intelligence, neural networks, intellectual property objects, protection of authors' rights, modern technologies in law

Введение. Развитие технологий искусственного интеллекта (далее – ИИ) и нейросетевых ресурсов в современной действительности поражает своей стремительностью и размахом, проникая во все сферы жизнедеятельности. Открывая новые перспективы и расширяя возможности, данные технологии ставят новые вопросы, требующие не только вдумчивых ответов, но и обоснованных решений, в том числе на законодательном уровне.

Одним из таких вопросов является возможность защиты объектов интеллектуальной собственности, созданных с использованием ИИ-технологий.

Часть четвертая Гражданского кодекса Российской Федерации [3] (далее – ГК РФ) относит к числу объектов интеллектуальной собственности широкий спектр результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации юридических лиц, товаров, работ, услуг и предприятий (ст. 1225 ГК РФ), презюмируя гарантированность охраны интеллектуальной собственности законом.

Право интеллектуальной собственности значительным образом укрепляет свои позиции и свою значимость в общем контексте регулирования гражданско-правовых отношений, в силу той цифровой трансформации, которая происходит в настоящее время: видоизменение общественных отношений в информационном пространстве, возникновение новых объектов интеллектуальной собственности, особенности создания как ранее известных гражданско-правовому регулированию объектов интеллектуальной собственности, так и новых и т. д.

С развитием интернет-технологий и социальных сетей, практически каждый из нас становится, в том или ином объеме, субъектом права интеллектуальной собственности, создавая и размещая в своих аккаунтах на различных сайтах, а также в социальных сетях авторские тексты, видеоролики, аудиозаписи и т. д.

Как отмечают в современных публикациях, даже «размещенные в социальных сетях авторские видеоролики – «рилсы», «истории» и т. д. – это тоже объект права интеллектуальной собственности, причем качественно новый. Голосовые сообщения, широко распространенные в различных соцсетях и мессенджерах, также могут выступать в подобном качестве. Даже обыкновенные текстовые посты в социальных сетях подпадают под регулирование права интеллектуальной собственности» [2. С. 306].

С развитием ИИ-технологий и популяризацией генеративных нейросетей, позволяющих создавать содержательные тексты, детализированные изображения и видеоролики, проблематика права интеллектуальной собственности перешла на качественно иной уровень: ключевой вопрос, который начал беспокоить большую часть граждан, использующих ИИ и нейросети в своей профессиональной и (или) творческой деятельности, касается определения автора произведения, созданного с помощью нейросетевых технологий и возможности защиты прав на данное произведение.

Основная часть. В соответствии с ч. 1 ст. 1228 ГК РФ, автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. При этом не признаются авторами результата интеллектуальной деятельности граждане, не внесшие личного творческого вклада в создание такого результата.

Данная гражданско-правовая норма является отправной точкой понимания того, кто может, а кто не может являться автором произведения, выступающего в качестве объекта интеллектуальной собственности.

Тем не менее специфика работы нейросетевых технологий, которые опосредуют создание готового объекта от запроса пользователя и до конечного результата (в виде текста, графики, аудио, видео и т. д.), не вполне «вписывается» в существующую нормативную и научную концепцию, заставляя ученых и практиков дискутировать о том, кого и в каком случае следует признавать автором произведения, созданного с помощью ИИ.

Условно, имеющиеся подходы можно свести к нескольким основным позициям, отражающим авторский взгляд на данную проблему.

1. **ИИ является автором произведения.** Несмотря на кажущуюся абсурдность данной крайне эксцентричной позиции, есть и ее сторонники. В частности, несколько лет назад за рубежом получило достаточно широкий резонанс дело, связанное с попыткой доктора Стивена Талера подать патентные заявки, в которых в качестве изобретателя фигурировала нейросетевая программа DABUS, разработчиком которой являлся Талер. Пройдя через ряд судебных процессов, Стивен Талер все же был признан Австралийским судом владельцем патентов, а изобретателем была признана разработанная им система DABUS, чего он, собственно, и добивался [1].

Тем не менее на данный момент в большинстве юрисдикций суды придерживаются традиционных подходов и трактовок, что не позволяет признавать за ИИ законные права.

Как резонно замечают отдельные исследователи, «искусственный интеллект существует в киберпространстве и, соответственно, как неодушевленный объект нематериального мира не может являться субъектом …» [12. С. 260].

Данный подход является фундаментальным, применительно к российскому правовому регулированию, что исключает возможность судебных решений такого рода.

В основном, в науке обсуждается лишь возможность признания наличия авторских прав у: владельца (создателя) нейросетевого ресурса, либо у пользователя данного ресурса. Отдельные исследователи рассматривают также возможность наличия соавторства между указанными субъектами [5. С. 100].

2. **Никто не является автором, если произведение создано с помощью ИИ.** Также можно выделить позицию, в соответствии с которой результат, сгенерированный ИИ-сервисом не может рассматриваться в качестве результата интеллектуальной деятельности и не подлежит правовой охране.

Тем не менее данная позиция выглядит не менее ущербной, чем ранее названная позиция, при которой авторские права на произведение закрепляются за ИИ.

Такой взгляд на статус материалов, полученных пользователем в результате работы с системой, не соответствует практической сути складывающихся отношений в данной сфере. При этом интересы участников данных отношений лишаются адекватной правовой защиты.

Очевидно, что такой подход не устроит пользователей ИИ-сервисов, а таковых с каждым днем становится все больше и больше – на данный момент только в Google Play количество скачиваний популярного ИИ-приложения «Шедеврум» от «Яндекс», работающего на базе нейросети «ЯндексАРТ», достигло более 10 млн.

Законодательное регулирование должно в максимальной мере соответствовать потребностям общественного прогресса на текущем этапе развития, отвечая взглядам общества на меру должного и справедливого.

Помимо этого, нормативное регулирование должно быть системным и не противоречить существующим базовым концептуальным подходам. В противном случае возникает дисбаланс, который вредит стабильности правового регулирования и развитию соответствующих общественных отношений. Игнорирование возникшего общественного запроса в плане обеспечения прозрачного и понятного регулирования по данному вопросу крайне нежелательно. Поэтому рассматриваемый подход в оценке авторства нейросетевых генераций следует признать несостоятельным.

3. **Владелец (создатель) ИИ-ресурса является автором произведения.** Такого рода позиция также может иметь место быть, учитывая то, что творческий результат объективно возникает как следствие использования, соответствующего ИИ-сервиса его пользователем.

Тем не менее нельзя смешивать авторские права на технологию, на основе которой работает сервис, с правами на результаты использования сервиса. Безусловно, разработчик ИИ-сервиса обладает авторскими правами на созданную им технологию – программное обеспечение, на котором работает нейросетевой ресурс. Но ставить «знак равенства» между технологическим решением и результатом использования данного технологического решения никак нельзя.

В противном случае творческий результат использования любого графического редактора (например, Adobe Photoshop) «автоматически» становился бы интеллектуальной собственностью компании разработчика данного ПО. Можно пойти в аналогиях еще дальше: авторские права на результат работы в текстовом редакторе Microsoft Word (в виде рассказа) не могут принадлежать никому другому, кроме как непосредственному автору данного произведения, воплотившему свой творческий замысел в литературном сюжете. Во всех обозначенных случаях, программное обеспечение используется автором в качестве инструмента – это достаточно очевидно и вряд ли подлежит сомнению.

Кроме того, в соответствии с ч. 1 ст. 1228 ГК РФ, не признаются авторами результата интеллектуальной деятельности «граждане, не внесшие личного творческого вклада в создание такого результата, в том числе оказавшие его автору только техническое, консультационное, организационное или материальное содействие или помощь…»

В данном случае предоставление ИИ-сервиса, способного воплотить задумку пользователя в виде готового объекта авторских прав, можно объективно расценивать, как организационно-техническое содействие автору результата интеллектуальной деятельности, не влекущее возникновение авторства.

Таким образом, идея наделения правами автора владельца (создателя) нейросетевого ресурса, работающего на основе генеративного ИИ, является несостоятельной как с точки зрения логики, так и с позиции действующего гражданско-правового регулирования.

4. **Пользователь ИИ-ресурса является автором произведения.** Данная позиция закономерно является самой обсуждаемой. В условиях стремительного развития ИИ-технологий и востребованности визуализаций практически во всех сферах, генерация изображений и видео является одной из наиболее востребованных ИИ-функций для пользователей. Кроме того, использование контента не ограничивается некоммерческими целями – его объем в рекламных материалах и медиапространстве в целом стремительно растет. По вполне понятным соображениям, среднестатистический пользователь нейросети считает себя автором сгенерированного визуального контента.

Помимо этого, ряд активных пользователей ИИ-сервисов считают себя владельцами сформулированных ими запросов (промптов), особенно когда речь идет о сложных лексических конструкциях, описывающих своего рода «техническое задание» для генеративной нейросети. Но об этом чуть позже.

В концептуальном плане человек, осуществляющий посредством работы в ИИ-сервисе создание произведения, является наиболее очевидным претендентом на роль автора: он является инициатором генерации, является автором идеи, которая закладывается в текст запроса, адресованного нейросети, и является тем, кто получает от ИИ-сервиса готовый результат генерации, сохраняя таковой в своем аккаунте, на своем устройстве и т. д.

Вопрос о соавторстве пользователя и владельца нейросетевого ресурса также не может быть решен положительно, поскольку во всех случаях, программное обеспечение используется автором-пользователем в качестве инструмента, то есть, имеет место техническое содействие со стороны владельца такого ресурса в достижении креативного результата. Данный факт исключает соавторство в силу прямого указания законодателя.

Как уже было сказано ранее, законодатель, при определении результата интеллектуальной деятельности исходит из презумпции того, что это – результат «творческого труда» автора (ч. 1 ст. 1228 ГК РФ).

Пленум Верховного Суда РФ, разъясняя соответствующие положения части четвертой ГК РФ в тексте Постановления от 23.04.2019 № 10 [9], исходит из того, что в качестве объекта авторского права (подлежащего охране) может рассматриваться только тот результат, который создан творческим трудом.

Соответственно, основной вопрос, который «стоит на повестке дня» применительно к разрешению вопроса об авторстве пользователя ИИ-ресурса, состоит в том, можно ли рассматривать полученный результат в качестве результата «творческого труда» данного индивида?

Обратим внимание на то, что в вышеупомянутом Постановлении Пленума ВС РФ № 10 подчеркивается, что «творческий характер создания произведения не зависит от того, создано произведение автором собственноручно или с использованием технических средств. Вместе с тем результаты, созданные с помощью технических средств в отсутствие творческого характера деятельности человека … объектами авторского права не являются» (п. 80 Постановления).

В словаре русского языка категория «творческий» определяется, как «созидательный, самостоятельно создающий что-нибудь новое, оригинальное» [6. С. 687].

Генерируемые изображения, видео и т. д. не являются копированием или «клонированием» уже имеющихся «чужих» результатов интеллектуальной деятельности, несмотря на то что генеративные ИИ-системы обучаются на огромных массивах информации, включающей разнообразные авторские графические материалы. Всякий раз нейросеть генерирует изображение или видео «с нуля», буквально формируя изображение из «цифрового хаоса». То есть формально каждая новая генерация по запросу пользователя (промпту) будет обладать свойством оригинальности и новизны – один и тот же пользовательский запрос не приводит к генерации одинаковых креативов. Однако полученные при этом результаты могут быть *похожими* друг на друга.

Также следует заметить, что мы не ведем речь о генерации контента в автономном режиме – мы рассматриваем типичную ситуацию, при которой инициатором, координатором и конечным получателем генерации выступает конкретное лицо: пользователь.

Здесь стоит учесть, что в Постановлении ВС РФ № 10 сделана важная оговорка: «само по себе отсутствие новизны, уникальности и (или) оригинальности результата интеллектуальной деятельности не может свидетельствовать о том, что такой результат создан не творческим трудом и, следовательно, не является объектом авторского права» (п. 80 Постановления).

Фактически подлежит охране практически любой результат интеллектуальной деятельности, который обнародован конкретным лицом, независимо от использования в данном произведении неуникальных и доступных для независимого создания идейных и иных составляющих.

Также заслуживает внимания вопрос о том, как быть, если запрос пользователя будет содержать в себе указание на чужой результат интеллектуальной деятельности? Например, если пользователь попытается сгенерировать изображение с популярными анимационными персонажами и т. д.?

В соответствии с уже неоднократно упоминаемой позицией Пленума ВС РФ, персонаж произведения, как «совокупность описаний и (или) изображений того или иного действующего лица в произведении», в принципе, обладает охраноспособностью в качестве объекта авторского права, если имеются индивидуализирующие его характеристики, «в силу которых действующее лицо произведения является узнаваемым даже при его использовании отдельно от всего произведения в целом» (п. 82 Постановления).

Другими словами, создание генераций с чужими объектами авторских прав создает неправомерное посягательство на чужие интеллектуальные права

и все связанные с этим риски принимает на себя автор произведения, сгенерированного в ИИ-сервисе. Кстати, данный аспект, наряду с иными, не менее важными вопросами, касающимися сгенерированного с помощью ИИ контента, содержится в пользовательских соглашениях, соответствующих ИИ-сервисов, определяя границы допустимого. В тех самых соглашениях, которые 99,9 % пользователей не читают, но безоговорочно принимают на этапе регистрации в сервисе.

Так, в Пользовательском соглашении об использовании мобильного приложения "GigaChat" от компании «Сбер» прямо указано: «Используя Сгенерированный Контент, Пользователь принимает на себя все риски, в том числе связанные с нарушением исключительных прав третьих лиц» [7].

Соответственно, пользователь должен сам предпринимать необходимые и достаточные меры, направленные на недопущение нарушения интеллектуальных прав иных лиц.

Какие выводы из существующего гражданско-правового регулирования, а также позиции Пленума ВС РФ, обозначенных выше, мы можем сделать?

Создание пользователем ИИ-сервиса изображения, видеоролика и т. д. с помощью программно-технического решения, предоставленного владельцем данного сервиса, правомерно рассматривать в качестве охраняемого законом объекта авторского права.

При этом сохраняется презумпция того, что автором результата ИИ-генерации выступает конкретный пользователь сервиса, при условии, что полученный результат интеллектуальной деятельности:

– содержит признаки творческого вклада данного пользователя (авторский замысел, содержащийся в запросе; выборка наилучшего результата, в максимальной мере отражающего задуманное, из ряда последовательных генераций и т. д.);

– не посягает на чужие охраняемые авторским правом результаты интеллектуальной деятельности (не воспроизводит части чужих произведений, персонажей и т. д.).

Как в зарубежной, так и в отечественной правоприменительной практике уже возникают ситуации, требующие защиты авторских прав на результаты интеллектуальной деятельности, созданные с помощью ИИ. Как правило, позиция истца строится на доказывании наличия творческого вклада в создание объекта интеллектуальной собственности. В том случае, когда такая позиция находит убедительные аргументы, суд удовлетворяет заявленные исковые требования, признавая право на защиту нарушенных авторских прав истца.

Так, Арбитражный суд г. Москвы удовлетворил исковые требования истца [10], связанные с незаконным использованием в сети Интернет аудиовизуального произведения, правообладателем которого он является.

Ответчик обратился в арбитражный суд с апелляционной жалобой, однако его доводы о том, что созданный видеоролик не является объектом авторского права по причине использования технологии Deep-fake были признаны несостоятельными: «монтаж исходных материалов видеоролика посредством технологии Deep-fake сам по себе не свидетельствует о том, что видеоролик доступен

для свободного использования (без согласия правообладателя), или о том, что группа лиц, обеспечившая написание сценария видеоролика, видеосъемку, его аудиосопровождение, не внесли личный творческий вклад в создание видеоролика и не признаются его авторами» [8].

Суд апелляционной инстанции оставил апелляционную жалобу по вышеназванному решению без удовлетворения.

В целом механизмы защиты рассматриваемых объектов интеллектуальной собственности, сгенерированных с помощью ИИ аналогичны защите прав на любые другие объекты интеллектуальной собственности.

А теперь рассмотрим вопрос о том, может ли рассматриваться запрос пользователя (промпт) в качестве результата интеллектуальной деятельности, претендующего на охрану в рамках авторского права?

Ответ будет следующим: в обычных условиях – нет, поскольку типичный запрос представляет собой лаконичный набор характеристик, определяющих пожелания и авторскую идею пользователя, а идеи, как четко следует из позиции законодателя, обозначенной в ч. 5 ст. 1259 ГК РФ, не являются объектами авторского права.

Компания «Яндекс», применительно к упомянутому ранее ИИ-сервису «Шедеврум», исходит из отсутствия правовой охраны пользовательских запросов, что указано в п. 3.2 Условий использования сервиса «Шедеврум»: «использование сервиса предполагает безвозмездную и безотзывную неисключительную лицензию на использование Запроса» [11].

Гипотетически исключение могут составлять объемные по содержанию и сложные по структуре авторские запросы, обладающие сюжетом и иными свойствами отдельного художественного произведения – литературной миниатюры. В таком виде пользовательский запрос может претендовать на роль объекта авторского права, *но не как промпт,* а как художественное произведение, *используемое в качестве промпта.*

Данная позиция представляется наиболее последовательной и убедительной, будучи основанной на существующей концепции авторского права, «приложенной» к инновационным способам создания произведений.

Следующий вопрос: какими правами обладает автор произведения, созданного с помощью ИИ-сервиса (мы уже пришли к выводу о том, что таковым мы «по умолчанию» считаем пользователя сервиса)?

Может ли он использовать результат генерации по своему усмотрению, в том числе в коммерческих целях? Могут ли иные лица использовать результат его интеллектуальной деятельности в своих целях без согласия автора?

Ответы на эти важные с практической точки зрения вопросы также содержатся в пользовательских соглашениях, соответствующих ИИ-сервисов.

Так, в рамках Условий использования сервиса «Шедеврум» указано, что пользователь вправе использовать контент (как сгенерированный им самим, так и другими пользователями сервиса) в личных некоммерческих целях с соблюдением правил сервиса и действующего законодательства. Любое коммерческое использование контента возможно только при условии предварительного согласования с Яндексом (п. 3.3 Условий).

Анализируемый документ содержит презумпцию возможности использования любого, сгенерированного и опубликованного пользователями в сервисе контента «Яндексом» в любых целях и любыми способами по своему усмотрению (п. 3.3 Условий).

То есть, априори, сервис имеет некоммерческую развлекательную направленность и в данном режиме предоставляется пользователям на безвозмездной основе.

Однако коммерческое и иное законное использование сервиса также возможно, на но условиях платной подписки, что оговорено в отдельном документе, именуемом Дополнительные опции: «Пользователь вправе использовать материалы, созданные с использованием Сервиса, в коммерческих целях, без предварительного согласования с Яндексом» [4].

Владелец ИИ-сервиса "GigaChat" в пользовательском соглашении вообще ничего не говорит о возможных целях использования сгенерированного контента, но в п. 4.3.1 упоминает запрет на использование приложения для противоправных целей. Тем не менее, в отличие от пользовательского соглашения «Шедеврум», где отсутствуют четкие указания на авторство пользователя, относительно сгенерированного контента, в пользовательском соглашении «GigaChat» наоборот прямо указывается, что: «Пользователь, использующий Приложение, является обладателем исключительного права на Сгенерированный Контент, созданный на основании Запроса Пользователя, с момента его создания» (п. 5.3 Пользовательского соглашения).

Таким образом, границы возможного использования изображений и иных креативов, созданных в соответствующих ИИ-сервисах, включая коммерческое использование, необходимо уточнять, путем изучения пользовательских соглашений, чтобы действовать в рамках правил, лежащих в основе именно того технологического решения, которым Вы собираетесь воспользоваться.

Заключение. Таким образом, опираясь на изложенное, можно сделать уверенный вывод о необходимости дополнительного гражданско-правового регулирования анализируемого спектра вопросов в целях исключения противоречивого и непоследовательного толкования как со стороны пользователей генеративных ИИ-сервисов, так и со стороны правоприменителя.

Такое регулирование может быть создано путем внесения изменений в текст ч. 1 ст. 1228 ГК РФ, а также ст. 1257 ГК РФ.

В новой редакции ч. 1 ст. 1228 ГК РФ может выглядеть следующим образом: «1. Автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат, включая случаи использования для создания результата интеллектуальной деятельности сервисов, работающих на основе технологий искусственного интеллекта».

В новой редакции ст. 1257 ГК РФ может быть сформулирована так: «Автором произведения науки, литературы или искусства признается гражданин, творческим трудом которого оно создано, включая случаи использования для создания произведения сервисов, работающих на основе технологий искусственного интеллекта. Лицо, указанное в качестве автора на оригинале или эк-

земпляре произведения либо иным образом в соответствии с пунктом 1 статьи 1300 настоящего Кодекса, считается его автором, если не доказано иное».

Данное законодательное решение может позволить создать принципиальную правовую определенность в отношение статуса результатов интеллектуальной деятельности, создаваемых пользователями сервисов, работающих на основе технологий искусственного интеллекта. При этом различные детали и особенности дальнейшего использования результатов, полученных гражданами посредством работы с ИИ-сервисом, могут быть уже урегулированы в рамках соответствующих пользовательских соглашений.

Учитывая инновационный характер деятельности, связанной с использованием ИИ-сервисов, их изменчивость, обусловленную бурным поступательным развитием данных технологий, соответствующие правоотношения также будут продолжать развиваться. Задача законодателя в данном ключе состоит в динамичном, своевременном и адекватном реагировании на данные изменения общественного и технологического прогресса в целях создания оптимального и справедливого баланса интересов участников анализируемых отношений.

Список литературы

1. I’m sorry Dave I’m afraid I invented that: Australian court finds AI systems can be recognised under patent law. URL: https://www.theguardian.com/technology/2021/jul/30/im-sorry-dave-im-afraid-i-invented-that-australian-court-finds-ai-systems-can-be-recognised-under-patent-law (дата обращения: 07.09.2025)
2. Аламова С. М. Основные тенденции развития права интеллектуальной собственности в современном мире // Право и государство: теория и практика. 2025. № 1. С. 305-308.
3. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // СЗ РФ. 2006. № 52 (1 ч.). Ст. 5496.
4. Дополнительные опции от 19.08.2025 г. URL: https://yandex.ru/legal/yandex_plus_opzii_list/ru/ (дата обращения: 07.09.2025)
5. Кантемиров Р. М. Критерии возникновения соавторства при создании произведений с использованием генеративного искусственного интеллекта // Актуальные проблемы российского права. 2025. Т. 20, № 6. С. 97-110.
6. Ожегов С. И. Словарь русского языка: Ок. 57 000 слов / под ред. Н.Ю. Шведовой. М.: Рус. яз., 1987. 797 с.
7. Пользовательское соглашение об использовании мобильного приложения «GigaChat». URL: https://cdn-app.sberdevices.ru/misc/0.0.0/assets/gigachat-web/6b77ba1b_license.html (дата обращения: 07.09.2025)
8. Постановление Девятого арбитражного апелляционного суда от 08.04.2024 № 09АП-642/24 по делу № А40-200471/2023 // СПС «Консультант плюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&cacheid=448272ACFC8391255B6E4D997C79FEC8&mode=searchcard&base=MARB&n=2651955&BASENODE=IiIiMiwyMDIsQUFTIiIsIiIyLDIwMCxBUyIiLCIiMiwyLEFSQiIiIg&rnd=TsfrAQ#8ckd6wUiwXSiAnPQ (дата обращения: 07.09.2025)

9. Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // Бюллетень Верховного Суда РФ. 2019. № 7.

10. Решение Арбитражного суда г. Москвы от 30.11.2023 по делу № А40-200471/23 // СПС «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/409465965/?ysclid=mf9jtcidab639388078 (дата обращения: 07.09.2025).

11. Условий использования сервиса «Шедеврум» от 24.06.2025 URL: https://yandex.ru/legal/shedevrum_termsofuse/ru/ (дата обращения: 07.09.2025).

12. Шевчук А. А. Особенности создания объектов авторских прав с использованием искусственного интеллекта // Вопросы российской юстиции. 2025. № 37. С. 256-262.

УДК 004.934

М. Т. Мурадов,
Институт телекоммуникаций и информатики,
г. Ашхабад, Туркменистан

Нейросетевой речевой синтез

Аннотация. Представленная научная статья посвящена исследованию области распознавания речи как одной из ключевых задач искусственного интеллекта. В работе анализируются современные подходы к распознаванию речи, основанные на статистических методах и системах искусственного интеллекта, включая скрытые марковские модели и нейронные сети. Особое внимание уделяется преимуществам использования нейронных сетей в акустическом моделировании, таких как устойчивость к шуму и высокая производительность. В статье также рассматривается процесс обработки аудиосигнала, включающий сегментацию на кадры для обеспечения статистической стационарности. Отмечается значительный прогресс в нейросетевом речевом синтезе, позволяющий генерировать естественную и выразительную речь с различными характеристиками и открывающий широкие перспективы для практического применения в различных сферах, направленных на улучшение коммуникации, доступности и эффективности.

Ключевые слова: распознавание речи, искусственный интеллект, статистические методы, нейронные сети, акустическое моделирование, сегментация аудиосигнала, нейросетевой речевой синтез, применение речевых технологий

M. T. Myradov
Institute of Telecommunications and Informatics
(Ashgabat, Turkmenistan)

Neural network speech synthesis

Abstract. The presented scientific article is devoted to the study of speech recognition as one of the key tasks of artificial intelligence. The paper analyzes modern approaches to speech recognition based on statistical methods and artificial intelligence systems, including hidden Markov models and neural networks. Special attention is paid to the advantages of using neural networks in acoustic modeling, such as noise resistance and high performance. The article also discusses the process of audio signal processing, including frame segmentation to ensure statistical stationarity. There has been significant progress in neural network-based speech synthesis, which allows for the generation of natural and expressive speech with various characteristics and opens up broad prospects for practical applications in various fields aimed at improving communication, accessibility, and efficiency.

Keywords: Speech recognition, artificial intelligence, statistical methods, neural networks, acoustic modeling, audio signal segmentation, neural network speech synthesis, application of speech technologies

Распознавание речи – одна из основных задач систем искусственного интеллекта. Сюда входят достижения в различных областях, таких как компьютерная лингвистика и цифровая обработка сигналов. Все это направлено на облегчение выполнения поставленных задач. Однако результаты и функционирование таких систем не являются устойчивыми.

Анализ этих систем позволит получить представление о принципах их работы, существующих недостатках и направлениях улучшения качества результатов.

Все современные системы распознавания речи основаны на статистических методах, которые позволяют использовать математическую статистику и теорию вероятностей, что в свою очередь значительно повышает качество распознавания.

Основными методами автоматического распознавания речи являются скрытые марковские модели и системы искусственного интеллекта [1, 2]. Нейронные сети широко используются в современных подходах, поскольку они свободны от многих ограничений, присущих гауссовым методам, и обладают лучшими возможностями обобщения. Кроме того, акустические модели, основанные на нейронных сетях, более устойчивы к шуму и имеют лучшую производительность [2]. Для получения спектра исходного сигнала аудиосигнал обычно разбивается на сегменты определенной длины с шагом, позволяющим им уместиться в половине кадров.

Разделение кадров необходимо для представления полученных сигналов статистически стационарным образом. Обычно размер кадра составляет 20–40 мс, так как если он короче, то не содержит достаточно информации для качественного анализа, а если длиннее, то сигнал слишком сильно изменяется и аудиоинформация ухудшается.

Достижения в области нейросетевого речевого синтеза привели к значительному улучшению качества, естественности и выразительности синтезируемой речи. Современные модели способны генерировать речь с различными стилями, эмоциями и акцентами, что открывает широкие возможности для применения в различных областях, включая голосовых помощников, системы взаимодействия человека с компьютером, синтез аудиокниг, средства коммуникации для людей с ограниченными возможностями и многое другое.

Таким образом, польза распознавания речи заключается в улучшении коммуникации, доступности и эффективности в различных сферах жизни и работы. Она открывает новые возможности для людей с ограниченными возможностями, повышает производительность в бизнесе и способствует более эффективному образованию. Благодаря этой технологии, мы можем сделать нашу жизнь проще, удобнее и более продуктивной.

Список литературы

1. Маковкин К. А. Гибридные модели: скрытые марковские модели и нейронные сети, их применение в системах распознавания речи // Модели, методы, алгоритмы и архитектуры систем распознавания речи. М.: Изд-во «Вычислительный центр им. А. А. Дородницына РАН», 2006.

2. Гефке Д. А., Зацепин П. М. Применение скрытых марковских моделей для распознавания звуковых последовательностей // Известия Алтай. гос. ун-та. Барнаул, 2012.

УДК 34.01

И. Е. Титов,
LL.M., юрист,
Международная юридическая фирма
ADVANT Beiten

Правовая квалификация e-mail-адреса в качестве цифрового идентификатора

Аннотация. Настоящая статья посвящена сравнительно-правовому анализу e-mail-адреса в качестве цифрового идентификатора. E-mail-адрес стал сегодня неотъемлемым спутником для каждого второго жителя Земли. Тем не менее анализ российского и зарубежного законодательства показывает либо отсутствие правового определения термина «e-mail-адрес», либо наличие определений, которые отражают лишь техническую суть данного объекта. В результате анализа российского и зарубежного законодательства, судебной практики и доктринальных источников автор приходит к выводу о том, что e-mail-адрес следует квалифицировать как уникальный цифровой идентификатор электронного почтового ящика пользователя.

Ключевые слова: цифровой идентификатор, e-mail, адрес электронной почты, Германия, США, Россия, правовая охрана, коммерческое обозначение, оператор почтового сервиса

I. E. Titov,
LL.M., Lawyer,
International Law Firm ADVANT Beiten

Legal qualification of an e-mail address as a digital identifier

Abstract. The article presents a comparative legal analysis of an e-mail address as a digital identifier. The e-mail address has now become an indispensable companion for every second inhabitant of the Earth. However, an analysis of Russian and foreign legislation reveals either a lack of a legal definition of the term "email address" or the presence of definitions that reflect only the technical nature of this object. Based on the analysis of Russian and foreign legislation, judicial practice, and doctrinal sources, the author concludes that an e-mail address should be classified as a unique digital identifier of a user's electronic mailbox.

Keywords: digital identifier, e-mail, e-mail address, Germany, USA, Russia, legal protection, trade name, e-mail service provider

Введение. E-mail-адрес стал сегодня неотъемлемым спутником для каждого второго жителя Земли. Согласно статистическим данным исследовательской компании *The Radicati Group, Inc.* к концу 2025 года количество пользователей электронной почты превысит 4,5 миллиарда, при этом на протяжении последних пяти лет сохраняется стабильная тенденция на увеличение их количества на 3% ежегодно [14. С. 3].

При этом по мнению авторов журнала *Forbes*, как в бизнес-среде компании имеют множество e-mail-адресов для решения различных задач, также и частным лицам рекомендуется иметь не менее четырех адресов электронной почты: один – для финансовых операций, второй – для личной корреспонденции, третий – для шоппинга и регистрации в различных онлайн-магазинах, а четвертый – для взаимодействия с государством [11].

Подобное масштабное использование данного инструмента неизбежно влечет за собой необходимость правовой охраны и защиты адреса электронной почты и прав на него конкретного пользователя, а, следовательно, и ставит перед законодателем и правоприменителями вопрос правовой квалификации адреса e-mail.

Определение e-mail-адреса в качестве идентификатора. Законодательное определение e-mail-адреса (от англ. *Electronic mail* – электронная почта), в настоящее время в российском законодательстве отсутствует, хотя имеется законодательное определение «электронного сообщения», под которым понимается информация, переданная или полученная пользователем информационно-телекоммуникационной сети [1. П. 10 ст. 2].

В российской судебной практике адрес электронной почты определяется как «*уникальная запись, уникальность которой гарантируется специальными протоколами, разработанными в соответствии со стандартами. Данная запись идентифицирует почтовый ящик пользователя и сообщает онлайн-сервису, куда именно необходимо доставить сообщение и прикрепленные к нему файлы*» [5].

В свою очередь, в Соединенных Штатах Америки (далее – США) определение адреса электронной почты имеется в федеральном законодательстве. Согласно пункту 5 параграфа 7702 раздела 15 Кодекса США термин «адрес электронной почты» определяется как «*назначение (англ. "destination"), обычно выражаемое в виде строки символов, состоящей из уникального имени пользователя (обычно называемого "локальной частью" (англ. "local part") и ссылки на интернет-домен (обычно называемого "доменной частью" (англ. "domain part"), независимо от того, отображается она или нет, на которое может быть отправлено или доставлено сообщение электронной почты*» [15. § 7702(5)].

Как видно из данного определения, оно носит технический характер и не позволяет определить правовой природы адреса электронной почты.

Тем не менее, основываясь на законодательной дефиниции, можно выделить следующие ключевые элементы адреса электронной почты.

Во-первых, это локальная часть, представляющая собой имя пользователя. Профессор У. Мюллер обозначает ее как свободно выбираемый пользовате-

лем логин (нем. *Log-in-Namen*) [12. Rn. 76]. Это, в частности, справедливо для публичных сервисов электронной почты, например, Mail.ru или Gmail, где логин для входа в сервис совпадает с локальной частью зарегистрированного пользователем адреса электронной почты.

Во-вторых, это доменная часть, то есть собственно указание на доменное имя, которое согласно пункту 4 параграфа 7702 раздела 15 Кодекса США представляет собой «*буквенно-цифровое обозначение зарегистрированное или назначенное регистратором доменных имен, реестром доменных имен или иным органом по регистрации доменных имен в качестве части электронного адреса в сети Интернет*» [15. § 7702(4)].

Кроме того, проф. У. Мюллер выделяет третью часть адреса электронной почты – символ «@» (англ. *at symbol*, нем. *@-Zeichen*), который выступает разделителем локальной и доменных частей [12. Rn. 76] и имеет значение указания на расположение конкретного электронного почтового ящика или аккаунта пользователя на соответствующем доменном имени (англ. *located at*).

Американская компания "*Cloudflare, Inc.*", которая предоставляет услуги CDN (от англ. "*Content delivery network*" – сеть доставки содержимого) на своем официальном сайте определяет адрес электронной почты как «*уникальную последовательность символов, которая служит идентификации учетной записи электронной почты или так называемого "электронного почтового ящика", на который можно отправлять электронные сообщения и где их можно получать*» [10].

Профессор М. А. Рожкова относит адрес e-mail к онлайн-идентификаторам (сетевым, виртуальным, цифровым идентификаторам), который представляет собой «*уникальный электронный адрес, предназначенный для пользователей независимой службы отправки электронной почты*» [7. С. 41].

Что же именно идентифицирует адрес электронной почты?

Из приведенных выше определений адреса электронной почты следует, что адрес e-mail идентифицирует прежде всего электронный почтовый ящик или «пункт назначения» для соответствующего электронного письма, что соотносится в данном случае и с техническими целями служб по пересылке и получению электронных писем.

Руководствуясь предложенной проф. М. А. Рожковой классификацией идентификаторов на уникальные и родовые, следует заключить, что адрес e-mail относится к уникальным сетевым идентификаторам, поскольку позволяет установить конкретный объект – электронный почтовый ящик. В силу технических особенностей системы регистрации доменных имен (доменная часть адреса e-mail) и системы регистрации логинов – уникальных имен пользователей в сервисах электронной почты (локальная часть адреса e-mail), второго тождественного адреса электронной почты существовать не может.

Правовая охрана адреса e-mail в качестве идентификатора. Как отмечает проф. У. Мюллер адрес электронной почты может обладать функцией идентификации (нем. «*Kennzeichnungsfunktion*»), хотя у пользователя и не возникает самостоятельного права на обозначение, зарегистрированное в качестве такого адреса [12. Rn. 76], в отличие, например, от права на товарный знак, ко-

гда регистрация обозначения в качестве товарного знака влечет возникновение правовой охраны такого обозначения.

В то же время согласно устоявшейся судебной практике в Германии, адреса электронной почты могут получить правовую охрану, если выполнены условия их использования в качестве коммерческого обозначения (нем. *Geschäftskennzeichen*).

Чтобы получить правовую охрану в качестве коммерческого обозначения такие идентификаторы должны использоваться в качестве указателей на происхождение (нем. *in herkunftshinweisender Weise*), т. е., указывать на предприятие-производителя товара или услуги, а не просто в качестве технического адреса [13]. Причем для этого не требуется, чтобы такой идентификатор использоваться в качестве основного коммерческого обозначения соответствующего предприятия.

В решениях по делам "soco.de" [8] и "seicom.de" [9] Федеральный верховный суд Германии указал, что при использовании обозначения исключительно в качестве адресной информации, потребитель будет полагать, что это указание – подобно номеру телефона – идентифицирует адресата, но не предназначено для идентификации происхождения товара или услуги.

Право использования соответствующего адреса электронной почты основано на договоре с оператором почтового сервиса, что предполагает возможное применение запретов и ограничений на уступку такого права требования третьим лицам.

В соответствии с пунктом 2.1. Пользовательского соглашения сервиса Почта Mail ООО «ВК» предоставляет пользователю доступ к сервису «Почта Mail» с возможностью создания персонального электронного почтового ящика с уникальным адресом электронной почты [3. П. 2.1]. При этом возможность обращения адресов электронной почты на вторичном рынке невозможна – установлен прямой запрет «продажи» то есть уступки права требования пользователя из договора с ООО «ВК» в отношении адреса электронной почты третьим лицам – в такой ситуации электронный почтовый ящик будет заблокирован без возможности к восстановлению [4. П. 8.3].

Аналогично согласно правилам сервиса Gmail «*покупать, продавать и перепродавать*» аккаунты, а, следовательно, и адреса электронной почты Gmail прямо запрещено [6].

Заключение. По результатам проведенного исследования мы можем сформулировать следующее определение e-mail-адреса: *e-mail-адрес представляет собой уникальный цифровой идентификатор электронного почтового ящика пользователя, представляющий собой последовательность символов, состоящий из локальной части, символа "@" и доменной части, используемый при отправке электронных сообщений*.

Право использования адреса e-mail основано на договоре с оператором почтового сервиса, то есть представляет собой право из договора. На возможность уступки данного права третьим лицам в договорах с операторами как правило установлен запрет, что, по сути, блокирует вторичный рынок адресов электронной почты публичных почтовых сервисов.

В то же время в ряде правопорядков, не исключена возможность приобретения адресом электронной почты правовой охраны в качестве коммерческого обозначения, если соответствующее обозначение используется не просто в качестве адресной информации, а в качестве указания на происхождение товаров или услуг от конкретного производителя.

Список литературы

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 07.09.2025).

2. Официальный комментарий ООО «ВК» в социальной сети «ВКонтакте». 28.09.2023. URL: https://vk.com/wall-81933640_4900422?ysclid=mf9qi49vmz491515244 (дата обращения: 07.09.2025).

3. Пользовательское соглашение сервиса Почта Mail. Редакция от 17.07.2025. URL: https://help.mail.ru/legal/terms/mail/ua/?ysclid=mf9o6bsagv577411917 (дата обращения: 07.09.2025).

4. Пользовательское соглашение сервисов Mail. Редакция от 02.12.2024. URL: https://help.mail.ru/legal/terms/common/ua/ (дата обращения: 07.09.2025).

5. Постановление Третьего арбитражного апелляционного суда от 05.06.2017 по делу № А74-9641/2016. URL: https://kad.arbitr.ru/Document/Pdf/ce4c455e-9548-49a0-a8c3-beae465e659d/0708ca26-0d27-491b-938a-abd769fb81bc/A74-9641-2016_20170605_Postanovlenie_apelljacionnoj_instancii.pdf?isAddStamp=True (дата обращения: 07.09.2025).

6. Правила программы Gmail. https://www.google.com/gmail/about/policy/ (дата обращения: 07.09.2025).

7. Рожкова М. А. Нематериальные объекты и имущественные права на них в системе абсолютных прав: монография. М.: ГАУГН Пресс, 2024. 258 с. (серия “IP & Digital Law”). DOI 10.18254/S6049896-9-2.

8. BGH, Urteil vom 22.07.2004 – I ZR 135/01 (OLG Stuttgart, LG Stuttgart) // MMR Zeitschrift für IT-Recht und Recht der Digitalisierung. 2005. URL: https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fmmr%2F2005%2Fcont%2Fmmr.2005.171.1.htm&anchor=Y-300-Z-WRP-B-2005-S-340&readableType=1 (дата обращения: 07.09.2025).

9. BGH, Urteil vom 24.02.2005 – I ZR 161/02 (OLG Stuttgart, LG Stuttgart) // MMR Zeitschrift für IT-Recht und Recht der Digitalisierung. 2005. URL: https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fmmr%2F2005%2Fcont%2Fmmr.2005.761.1.htm&anchor=Y-300-Z-MMR-B-2005-S-761&readableType=2&VorgaengerDokumentStreffer3=Beschluss%20vom%2011.07.2005%20-%20NotZ%208%2F05&VorgaengerDokumentFullname=bibdata%2Fzeits%2Fmmr%2F2005%2Fcont%2Fmmr.2005.759.1.htm (дата обращения: 07.09.2025).

10. Cloudflare, Inc. What is email? Email definition. URL: https://www.cloudflare.com/learning/email-security/what-is-email/ (дата обращения: 07.09.2025).

11. Haber M. Why Every Person Needs At Least Four Email Accounts. Forbes. 13.02.2020. Updated 14.04.2022. URL: https://www.forbes.com/councils/forbestechcouncil/2020/02/13/why-every-person-needs-at-least-four-email-accounts/ (дата обращения: 07.09.2025).

12. Müller U. Vorbemerkung: Allgemeine Grundsätze des Kennzeichenrechts in der Kommunikationsbranche // In Spindler/Schuster. Recht der elektronischen Medien. 4. Auflage. 2019. URL: https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fspindlerschusterkorem_4%2Fmarkeng%2Fcont%2Fspindlerschusterkorem.markeng.vor1.p1.glvii.gl2.glb.htm&pos=7&hlwords=on (дата обращения: 07.09.2025).

13. OLG Hamburg: Verwendung eines unterscheidungskräftigen Zeichens als E-Mail-Adresse – PATMONDIAL // MMR Zeitschrift für IT-Recht und Recht der Digitalisierung. 2011. URL: https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fmmr%2F2011%2Fcont%2Fmmr.2011.324.1.htm&anchor=Y-300-Z-MMR-B-2011-S-324&readableType=2&VorgaengerDokumentStreffer3=Urteil%20vom%2009.02.2010%20-%2015%20U%20107%2F09&VorgaengerDokumentFullname=bibdata%2Fzeits%2Fmmr%2F2011%2Fcont%2Fmmr.2011.323.1.htm (дата обращения: 07.09.2025).

14. The Radicati Group, Inc. Email Statistics Report, 2021-2025. February 2021. URL: https://www.radicati.com/wp/wp-content/uploads/2020/12/Email-Statistics-Report-2021-2025-Executive-Summary.pdf (дата обращения: 07.09.2025).

15. 15 U.S. Code § 7702 – Definitions // Pub. L. 108–187, § 3, 16.12.2003, 117 Stat. 2700. URL: https://www.law.cornell.edu/uscode/text/15/7702#5 (дата обращения: 07.09.2025).

УДК 342.9

А. Н. Агарков,
аспирант,
Орловский государственный университет
имени И. С. Тургенева

Цифровая трансформация административной юстиции: вызовы для гарантий прав личности в свете новелл КОАП РФ

Аннотация. Статья посвящена комплексному анализу рисков для процессуальных гарантий прав личности, возникающих в связи с масштабной цифровизацией производства по делам об административных правонарушениях. Цель исследования – выявление коллизий между принципами эффективности и состязательности при использовании электронного документооборота, дистанционных технологий и фиктивных конструкций извещения по нормам Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ). Методология включает сравнительно-правовой анализ новелл КоАП РФ с подходами, закрепленными в Гражданском процессуальном кодексе Российской Федерации (далее – ГПК), Уголовно-процессуальном кодексе Российской Федерации (далее – УПК) и Кодексе административного судопроизводства Российской Федерации Российской Федерации (далее – КАС), а также изучение современной научной доктрины и правоприменительной практики. В результате выявлены системные проблемы «цифрового неравенства», ослабления права на защиту и автоматизма в оценке надлежащего извещения. Автором предложены конкретные меры законодательного и организационного характера, направленные на достижение баланса между оперативностью административного процесса и незыблемостью фундаментальных прав человека.

Ключевые слова: цифровизация правосудия, КоАП РФ, электронный документооборот, гарантии прав личности, надлежащее извещение, цифровое неравенство, административный процесс

A. N. Agarkov,
Postgraduate student, Orel State University named after I. S. Turgenev,

Digital transformation of administrative justice: challenges for the guarantees of individual rights in the light of the novels of the code of administrative offenses of the Russian Federation

Abstract. The article is devoted to a comprehensive analysis of the risks to the procedural guarantees of individual rights arising in connection with the large-scale digitalization of proceedings in cases of administrative offenses. The purpose of the

study is to identify collisions between the principles of efficiency and competitiveness when using electronic document management, remote technologies and fictitious structures of notification under the norms of the Code of Administrative Offenses of the Russian Federation. The methodology includes a comparative legal analysis of the novels of the Code of Administrative Offenses of the Russian Federation with the approaches enshrined in the Code of Civil Procedure, the Code of Criminal Procedure and the Code of Administrative Procedure of the Russian Federation, as well as the study of modern scientific doctrine and law enforcement practice. As a result, systemic problems of the "digital divide", weakening of the right to defense and automatism in the assessment of proper notification are identified. The author proposes specific measures of a legislative and organizational nature aimed at achieving a balance between the efficiency of the administrative process and the inviolability of fundamental human rights.

Keywords: digitalization of justice, Code of Administrative Offenses of the Russian Federation, electronic document management, guarantees of individual rights, proper notification, digital inequality, administrative process

Введение. Современный этап развития российской правовой системы неразрывно связан с ее активной цифровой трансформацией. Проникновение цифровых технологий в сферу правосудия и публичного администрирования – общемировой тренд, отвечающий вызовам времени. В Российской Федерации этот процесс приобрел системный характер после принятия целого ряда основополагающих нормативных актов, в том числе «революционного» Федерального закона от 7 апреля 2025 года № 59-ФЗ [5], внесшего поистине революционные изменения в КоАП РФ [3]. Данный закон, по сути, ознаменовал новый этап, закрепив комплексное регулирование электронного документооборота, дистанционного участия в процессуальных действиях и использования информационных систем на всех стадиях производства – от составления протокола до исполнения постановления.

Однако стремительная цифровизация столь чувствительной сферы, как административная ответственность, где одной из сторон всегда выступает властный субъект, объективно порождает серьезное правовое напряжение. Законодатель, пытаясь создать гибкую и современную систему, вынужден искать непростой компромисс между целями эффективности, оптимизации и безусловного соблюдения гарантий прав личности. К сожалению, как показывает практика и доктринальный анализ, этот баланс не всегда достигается [7, 9]. Актуальность темы обусловлена необходимостью осмысления новых рисков и выработки механизмов их минимизации. Целью настоящего исследования является выявление системных проблем и коллизий, возникающих при использовании информационных систем в административном процессе на основе новелл КоАП РФ, и разработка путей их решения через призму сравнительного анализа со смежными отраслями процессуального права.

Основная часть

1. Сравнительно-правовой анализ ключевых новелл КоАП РФ и системные риски. Поправки, внесенные в КоАП РФ Законом № 59-ФЗ, носят

комплексный характер. Их сравнительно-правовой анализ с нормами других процессуальных кодексов позволяет выявить как прогрессивные черты, так и системные риски для реализации прав граждан и предпринимателей.

Ключевой особенностью новой редакции КоАП РФ является закрепление в статьях 24.8 и 24.9 множественности каналов для подачи и получения процессуальных документов. В их число входят Единый портал госуслуг (ЕПГУ), личные кабинеты юрлиц и ИП на сайтах госорганов, региональные порталы, системы межведомственного электронного документооборота (СМЭВ), а также традиционные способы – почтовая связь и личное вручение.

В отличие от более унифицированного подхода КАС РФ (ст. 125) и ГПК РФ (ст. 35, 131), которые ориентированы на централизованные платформы (ГАС «Правосудие», ЕПГУ), множественность каналов, введенная в КоАП РФ, по-видимому обусловлена желанием законодателя охватить не только взаимодействие с судом, но и с огромным массивом несудебных органов власти (более 60 субъектов административной юрисдикции). Представляется, что такой подход создает, так называемый «эффект лабиринта» для гражданина или малого бизнеса, поскольку ввиду недостаточного уровня не только цифровой, но и юридической грамотности граждан, высок риск ошибиться с выбором платформы, не отследить поступление документа, пропустить процессуальный срок и в итоге лишиться возможности защиты. Налицо системный дисбаланс («асимметрия») между властью и частным лицом: государственный орган зачастую использует мощные корпоративные СМЭД и имеет штатных IT-специалистов, в то время как частное лицо *de facto* ограничено техническими и информационными ресурсами ЕПГУ, доступ к которому для многих остается проблематичным [6. С. 207]. Данная проблема усугубляется общим «цифровым неравенством» (digital divide) внутри страны, которое проявляется в дисбалансе уровней развития цифровой инфраструктуры и компетенций между регионами и даже между крупными и малыми городами [11. С. 90]. Таким образом, гражданин или предприниматель из малого города сталкивается с двойной нагрузкой: как с общесистемным недостатком качественных цифровых сервисов в своем регионе, так и с изначальной сложностью и неравенством цифровых инструментов диалога с властью, заложенными в новом процедурном регулировании КоАП РФ.

Наиболее дискуссионным и вызывающим тревогу с точки зрения гарантий прав личности нововведением является фикция надлежащего извещения, закрепленная в ч. 6 ст. 24.9 КоАП РФ. Согласно ей, документ считается полученным, в частности, с момента входа пользователя в личный кабинет на ЕПГУ, региональном портале, официальном сайте суда и т.д. (п. 9, 11 ч. 6), при этом, в случае невхода в течение 7 дней – направляется бумажная копия (ч. 8 ст. 24.9). Для сравнения, КАС РФ (ст. 96) связывает фикцию получения с фактом размещения документа в личном кабинете и истечением разумного срока, а УПК РФ (ст. 474.1) **ставит фикцию получения в зависимость от предварительного и конкретного согласия лица** на электронное взаимодействие, что обеспечивает максимальные гарантии.

Таким образом, изложенная законодателем в КоАП модель, **уступая по степени гарантий подходу УПК РФ** [4], несмотря на свои преимущества перед

КАС РФ [2], остается обременительной для гражданина, так как требует от него постоянного отслеживания всех потенциально возможных «личных кабинетов». Для **граждан, не обладающих высокой цифровой грамотностью или не имеющих постоянного доступа к интернет-ресурсам** (например, жители удаленных районов, социально незащищенные слои населения, лица престарелого возраста), которые могут не знать о самом существовании такого кабинета или испытывать технические трудности с доступом, это прямой путь к цифровому исключению (digital exclusion) и потере права на защиту в результате банального пропуска срока. Подобные риски цифрового исключения, отмечаемые исследователями в гражданском процессе [12], в административном процессе усугубляются из-за изначальной асимметрии отношений «гражданин – власть».

Проблема цифровизации затрагивает и реализацию права на защиту при дистанционных процедурах. Новая редакция статьи 28.2 КоАП РФ допускает беспрецедентную ситуацию, когда составление первичных документов, в том числе протокола об административном правонарушении, осуществляется дистанционно, с использованием систем видеоконференц-связи (ВКС) и веб-конференции, но без должных процессуальных гарантий. К примеру, уголовный процесс детально регламентирует проведение следственных действий (допроса, очной ставки, опознания) с использованием ВКС на стадии предварительного расследования, выделяя это в отдельную норму – статью 189.1 УПК РФ. Данная процедура обеспечивается силами государственных органов, гарантирует обязательное применение видеозаписи и предусматривает механизм фиксации хода действия и полученных показаний. В административном процессе аналогичное по сути действие (составление протокола) может быть проведено с использованием менее защищенных технологий веб-конференции, при этом **новеллы КоАП РФ не содержат императивного требования об обязании видеофиксации** подобного сеанса связи и приобщения ее записи к материалам дела. Данное обстоятельство ставит под сомнение возможность последующей проверки добровольности дачи объяснений, отсутствия давления на лицо и корректности процедуры. В свою очередь, КАС РФ и ГПК РФ [1] регулируют участие посредством ВКС и с использованием системы веб-конференции только в судебном заседании (ст. 142, 142.1 КАС РФ, ст. 155.1, 155.2 ГПК РФ), в связи с чем не содержат нормы, регламентирующие вышеуказанные досудебные процедуры, на которые можно было бы ориентироваться законодателю.

Таким образом, КоАП РФ становится уникальным кодексом, позволяющим дистанционно проводить ключевое первоначальное действие с использованием технологий, не обеспеченных адекватными процессуальными гарантиями достоверности. Это порождает серьезные риски, среди которых:

1. Формализация процедуры и психологическое давление на лицо в отсутствие привычной «кабинетной» обстановки.

2. Фактическая невозможность получить немедленную юридическую помощь защитника непосредственно в момент составления протокола.

3. Сложности в полноценном ознакомлении с материалами и заявлении ходатайств в режиме онлайн.

4. Вопросы к достоверности идентификации и конфиденциальности передаваемых данных при использовании публичных платформ для веб-конференций.

5. Невозможность проверить обстоятельства и условия составления протокола (было ли оказано давление, правильно ли лицу разъяснили его права, не было ли технических сбоев, исказивших смысл сказанного) в случае возникновения спора.

6. Техническая ненадежность, поскольку качество связи зачастую оставляет желать лучшего, а техническое оснащение органов власти повсеместно отстает от законодательных новаций, что приводит к срывам сессий, искажению информации и нарушению принципа непосредственности [10; 11. С. 90].

2. Предложения по совершенствованию электронного административного судопроизводства. На основе проведенного анализа представляется целесообразным предложить следующие меры, направленные на гармонизацию законодательства и усиление гарантий прав личности в условиях цифровизации.

В области законодательных инициатив, прежде всего, необходима унификация цифровых платформ путем закрепления на уровне закона приоритета ЕПГУ и ГАС «Правосудие» как основных и единых порталов для взаимодействия гражданина с государством по делам об административных правонарушениях. При этом иные способы, такие как СМЭВ, должны стать опциональными и дополнительными, а не альтернативными для властных субъектов. Также более рациональным представляется внедрение гибридной модели активного извещения, для чего требуется усовершенствовать пункты 9 и 11 части 6 статьи 24.9 КоАП РФ. Предлагается дополнить механизм фикции обязательным активным уведомлением о поступлении документа в личный кабинет. Фикция получения должна наступать не в момент входа пользователя и не в момент размещения документа, а по истечении короткого срока (например, 3–5 дней) с момента подтверждения доставки автоматического оповещения на заранее указанные лицом контакты. В качестве каналов оповещения должны использоваться SMS, push-уведомление в мобильном приложении Госуслуг или email. Ключевым условием должно стать право лица самостоятельно и безвозмездно выбирать и подтверждать предпочтительный канал для таких оповещений в настройках профиля ЕСИА (Единой системы идентификации и аутентификации). Только после подтверждения доставки уведомления и отсутствия реакции на него в течение более длительного разумного срока (например, 15 дней) должна запускаться процедура обязательной отправки бумажной копии традиционной почтой. Кроме того, важно закрепить процессуальные гарантии на досудебной стадии, внеся в статью 28.2 КоАП РФ прямые нормы. Они должны гарантировать право лица на защитника при проведении дистанционных процедур составления протокола, право на перерыв для конфиденциальной консультации с ним, а также детальный порядок заявления и фиксации возражений и ходатайств. Для обеспечения достоверности процедуры и возможности последующего контроля необходимо введение обязательной видеофиксации всего сеанса связи при составлении протокола с использованием ВКС или веб-конференции, что следует закрепить в КоАП РФ. Материалы видеозаписи должны храниться и предостав-

ляться суду по его требованию или ходатайству лица для проверки добровольности дачи объяснений, отсутствия давления и корректности процедуры. Эффективность данного механизма подтверждается многолетней практикой оформления административных материалов сотрудниками ДПС с обязательной видеофиксацией, что стало ключевой гарантией защиты прав граждан и законности действий должностных лиц.

В организационно-управленческой сфере предлагается создание системы технической и юридической поддержки через организацию на базе МФЦ или судов бесплатных консультационных пунктов и горячих линий для помощи гражданам и предпринимателям в работе с цифровыми сервисами КоАП РФ, включая помощь в получении электронной подписи. Параллельно требуется реализация государственных информационных кампаний о новых цифровых правах и обязанностях, а также проведение обязательных курсов повышения квалификации для судей и должностных лиц с акцентом на соблюдении прав человека и практике применения смежных кодексов (КАС, ГПК РФ).

Среди технологических решений ключевыми представляются активное внедрение биометрической идентификации с использованием Единой биометрической системы как более безопасной и удобной альтернативы простой электронной подписи для доступа к личным кабинетам и участия в онлайн-заседаниях, что частично нивелирует проблему цифрового неравенства, а также повышение юзабилити и доступности интерфейсов государственных порталов. Последнее необходимо реализовывать путем проведения обязательного юзабилити-тестирования с привлечением фокус-групп из разных социальных и возрастных категорий для обеспечения понятности и удобства сервисов для конечного пользователя.

Заключение. Проведенный анализ показывает, что, несмотря на значительный и прогрессивный шаг вперед, цифровизация административного судопроизводства в России выявила системные проблемы, связанные с обеспечением классических процессуальных гарантий прав личности. Основными рисками остаются усугубляющееся цифровое неравенство, уязвимость механизмов идентификации и несовершенство, а подчас и излишняя жесткость фиктивных конструкций надлежащего извещения.

Предложенные в статье меры – унификация платформ, гарантии доступа к технологиям, вариативности фиктивных конструкций и детализация процедурных гарантий – направлены на тонкую, но критически важную настройку созданной системы. Их реализация позволит достичь того самого неуловимого баланса между оперативностью и эффективностью административного процесса, с одной стороны, и соблюдением прав и свобод человека – с другой. Ведь именно это, а не голые технологические показатели, является конечной целью любого правового государства, претендующего на звание современного и справедливого. Дальнейшие исследования, несомненно, должны быть сконцентрированы на анализе первоначальной правоприменительной практики новых норм КоАП РФ и выработке единообразных подходов для судей и должностных лиц.

Список литературы

1. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. 2002. № 46. Ст. 4532.

2. Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ (ред. от 07.07.2025) // Собрание законодательства РФ. 2015. № 10. Ст. 1391.

3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 23.07.2025 с изм. и доп., вступ. в силу с 03.08.2025) // Российская газета, № 256, 31.12.2001.

4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 31.07.2025 с изм. и доп., вступ. в силу с 01.09.2025) // Собрание законодательства РФ. 2001. № 52 (ч. I). Ст. 4921.

5. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: федеральный закон от 07.04.2025 № 59-ФЗ // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru (дата обращения: 08.08.2025).

6. Абдульманова А.И. Проблемы цифровизации электронного судебного делопроизводства и принудительного исполнения судебных актов // International Journal of Humanities and Natural Sciences. 2024. Т. 10-1 (97). С. 205–211.

7. Алешкова И.А. Цифровизация и судебная деятельность: (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. 2022. № 3. С. 76–88.

8. Васильева Е.С. Влияние информационных технологий на становление и развитие судебной системы в Российской Федерации // Вестник Сургутского государственного университета. 2013. № 1. С. 76–79.

9. Гаймалеева А.Т. Цифровизация судебной системы: анализ тенденций развития процессуального законодательства (на примере проекта изменений в Гражданский процессуальный кодекс Российской Федерации) // Правовое государство: теория и практика. 2020. № 4 (62). С. 28–39.

10. Кожич И.С. Следственные действия путем использования систем видеоконференцсвязи // Молодой ученый. 2022. № 20 (415). С. 306-307.

11. Кузнецов А.А. Проблемы реализации цифровизации судопроизводства в современном информационном пространстве России // Образование. Наука. Научные кадры. 2022. № 2. С. 88–92.

12. Петрунин Н.В. Перспективы цифровизации судебной власти // Гуманитарные, социально-экономические и общественные науки. 2023. № 5. URL: https://cyberleninka.ru/article/n/k-voprosu-o-tsifrovizatsii-ugolovnogo-sudoproizvodstva (дата обращения: 03.09.2025).

УДК 347.9

О. А. Васючкова,
кандидат юридических наук, доцент,
Финансовый университет
при Правительстве Российской Федерации,
генеральный директор
автономной некоммерческой организации
«Научно-исследовательский кластер
в области науки, образования, права «РЕПУТАЦИЯ»

Цифровые технологии как средство устойчивого развития судебной системы в России

Аннотация. Целью настоящего исследования является анализ применения цифровых (коммуникационных) технологий в рамках взаимодействия субъектов гражданского оборота с судами в России, которые меняют и реформируют судебную систему в целом и обладают рядом значимых преимуществ, способных позитивно влиять на развитие общественных отношений в целом. В силу стремительного развития общественных отношений, цифровая модернизации деятельности судов, рассматривается автором как необходимость нашего времени для создания комфортной и безопасной социальной среды. Благодаря выбранной методологии познания (общенаучных и частно-научных методов исследования) автор выделяет ряд перспективных направлений анализируемых технологий, перечень которых необходимо расширять и распространять по всей территории нашей страны.

Ключевые слова: судебная деятельность, коммуникационные технологии, доступ к правосудию, технологический прорыв, комфортная среда

O. A.Vasyuchkova,
Candidate of Law,
Associate Professor,
Financial University under the Government of the Russian Federation,
General Director of the autonomous non-profit organization
"Scientific research cluster in the field of science, education, law "REPUTATION"

Digital technologies as a means of sustainable development of the judicial system in Russia

Abstract. The purpose of this study is to analyze the use of digital (communication) technologies in the framework of the interaction of subjects of civil turnover with the courts in Russia, which are changing and reforming the judicial system as a whole and have a number of significant advantages that can positively influence the development of public relations in general. Due to the rapid development of public relations and the digital modernization of the courts, the author considers it a necessi-

ty of our time to create a comfortable and safe social environment. Thanks to the chosen methodology of cognition (general scientific and private scientific research methods), the author identifies a number of promising areas of the analyzed technologies, the list of which needs to be expanded and disseminated throughout our country.

Key words: judicial activity, communication technologies, access to justice, technological breakthrough, comfortable environment

Введение. Информационные технологии играют значимую роль в общественных отношениях, влияя на качественные характеристики его развития и функционирования. Они проникают во все сферы нашей жизни, начиная от образования и заканчивая экономикой. Коммуникационные технологии стали неотъемлемой частью повседневной жизни людей и общества в целом, они способствуют ускорению обмена информацией, повышению эффективности процессов и созданию новых возможностей для взаимодействия и коммуникации, а специфика информатизации общества, влияет на государственное управление и развитие государства в целом» [11. С 74]. Таким образом, влияние информационных технологий выходит за рамки индивидуального использования и затрагивает важные аспекты государственного управления и социального развития в том числе сферу деятельности судов.

Цифровые технологии не только способствуют экономическому росту, но и создают новые формы взаимодействия и инноваций. Они развивают цифровую экономику, улучшают доступ к образованию и правосудию, а также помогают решать глобальные проблемы, включая экологические вызовы и социальное неравенство. Важно отметить, что изменения происходят не только в базисных сферах общественной жизни, таких как экономика, политика и технологии, но и в области коммуникативных процессов [10].

Доступ к информации в современном обществе становится неотъемлемым элементом для реализации потенциала каждого человека. Анализ изменений задач в образовании, в условиях становления информационного общества показывает, что современное образование становится основой для подготовки тех или иных специалистов, что подчеркивает важность качественного доступа к информации для формирования необходимых навыков и компетенций [9].

Основная часть. С целью экономического и социального развития Российской Федерации, обозначенные в Указе Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» (далее – Указ) [1] национальные цели, достигаются сформированными в Указе задачами. Некоторые из перечисленных в Указе задачи, такие как – комфортная и безопасная среда, цифровая трансформация государственного и муниципального управления, экономики и социальной сферы, выполнимы в рамках комплексного внедрения и использования цифровых технологий [8. С 105]. Внедрение цифровых технологий в правовое регулирование общественных отношений трансформирует их и определяет вектор технологического прорыва во всех сферах государственного управления, основанного на гибком подходе в каждой сфере.

В рамках национальной программы "Цифровая экономика Российской Федерации" (п. 2 разд. 2 "Паспорта национального проекта "Национальная программа "Цифровая экономика Российской Федерации", утв. Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7 [6], поставлена цель создать устойчивую и безопасную информационно-телекоммуникационную инфраструктуру высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств. Результатом достижения поставленных целей является технологический прорыв в деятельности судов, который достигается путем активного применения цифровых технологий и их масштабирования по всей территории нашей страны.

Коммуникационные или цифровые технологии, используемые в деятельности судов, стали частью процесса рассмотрения дел, фиксируя действия, не только происходящие в рамках судебного разбирательства (в частности – аудио протоколирование судебного заседания), но и действия, происходящие вне судебного процесса в рамках электронного взаимодействия. О перспективах и ожиданиях цифровых технологиях в деятельности судов говорят с 2020 г., определяя их позитивную роль в развитии судебной системы в целом [7. С 13].

Так, в соответствии с пунктами 5.3.3, 5.3.4 Концепции информатизации судов и системы Судебного департамента до 2030 года, утвержденной постановлением Президиума Совета судей Российской Федерации от 2 декабря 2019 г. № 785 (далее – Концепция) [2], внедрены и используются следующие технологии: суперсервис «Правосудие онлайн федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации», обеспечивающий подачу гражданами и организациями процессуальных документов в электронном виде через Единый портал государственных и муниципальных услуг; программные средства распознавания речи с автоматизированным формированием протокола судебного заседания с приложением аудио-, видеозаписи.

В основе цифровых коммуникаций лежат электронные способы передачи соответствующей информации. Традиционные способы получения информации в деятельности судов (письменной и устной) уходят в эпоху. Однако внедрение цифровых технологий не исключает применение традиционных способов передачи информации, а только предоставляет дополнительные возможности для тех, кто ценит время и деньги. Автор считает, что электронный способ передачи информации, информатизация процессов в деятельности судов подтверждает технологический прорыв и способствует устойчивому развитию судебной системы нашей страны.

Правовое регулирования информатизации деятельности судов осуществляется в соответствии с Федеральным законом от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» [3], а в отношении деятельности Верховного суда Российской Федерации Концепцией информатизации Верховного Суда Российской Федерации, утв. приказом Председателя Верховного Суда РФ от 15 февраля 2021 г. № 9-П [4].

Ключевыми средствами информатизации являются информационные системы, обеспечивающие деятельность судов.

В российском правосудии используются такие ключевые информационные системы как:

– ГАС «Правосудие» – единая автоматизированная система, объединяющая суды общей юрисдикции. Обеспечивает ведение дел, учет статистики и взаимодействие между судами;

– «Мой арбитр» – портал для подачи документов в арбитражные суды в электронном виде (ст. 125 АПК РФ). Позволяет отслеживать движение дела.

– «Картотека арбитражных дел» – публичный ресурс с информацией о делах (ст.228 АПК РФ). Позволяет проверять статус дел, скачивать судебные акты;

Официальные сайты судов [5] позволяют в электронном формате передавать и получать любую процессуальную информацию по различным делам. Комплекс видеоконференц-связи (онлайн-заседания) открывают доступ к правосудию вне зависимости территориального признака проживания стороны процесса.

Итак, коммуникационные технологии имеют ряд преимуществ, таких как осуществления открытого доступ к правосудию, к информации о деятельности судов, повышение эффективности судебной защиты прав и законных интересов граждан, организаций, органов государственной власти, повышение качества осуществления правосудия, доступ к анализу материалов судебных дел.

Доступ к правосудию обеспечивается возможностью дистанционно обратиться в суд в электронном виде, дистанционно получить информацию о судебном процессе, воспользоваться правом на дистанционное участие в судебных заседаниях, ознакомления с судебными делами в электронном формате и взаимным обменом информацией между судом и участниками процесса.

Доступ к информации о деятельности судов позволяет – предоставлять пользователям доступ к информационным ресурсам, включая Судебный портал, открыто и доступно находить нужную информацию о деятельности судов, рассчитывать на ее достоверность и своевременность предоставления, не вмешиваться в осуществление правосудия при предоставлении информации о деятельности судов.

Повышение эффективности судебной защиты прав и законных интересов граждан, организаций, органов государственной власти проявляется в повышение эффективности деятельности участия н снижение издержек участников судебного процесса посредством использования дистанционных форм участия в судопроизводстве (ВКС, онлайн-заседание), доступности и открытости правосудия (использования личного кабинета ЕПГУ, СЭД участников судебного процесса и т. д.).

Повышение качества осуществления правосудия достигается формированием единого цифрового пространства и совершенствованием электронного взаимодействия с использованием системы межведомственного электронного взаимодействия и системы межведомственного электронного документооборота.

Доступ к анализу материалов судебных дел позволяет просчитывать правовые риски (перспективу достижения цели), а формирование единой судебной практики способствует снижению судебных издержек и планированию способов оказания правовых услуг.

Список вышеизложенных автором преимуществ открыт и будет дополняться по мере совершенствования механизмов внедрения и использования цифровых технологий в деятельности судов. Судебная система в РФ развивается и совершенствуется, а цифровые технологии показали свою эффективность и полезность, а значит их масштабирование необходимо ускорить, так как они минимизируют фактические барьеры доступа к правосудию, снижают судебные (финансовые) издержки, дают возможность ускоренной коммуникации с судами по конкретным делам.

Все выше проанализированные преимущества влияют на развитие и совершенствование информационных технологий судебного документооборота и делопроизводства, судебной статистики, развитие и совершенствование информационных технологий общего документооборота и делопроизводства, модернизацию внутренней телекоммуникационной инфраструктуры судов, развитие видео-конференц-связи, развитие и совершенствование защиты информации, предоставляемой судами.

Заключение. Россия демонстрирует амбициозный подход к интеграции инноваций в судебную систему, что соответствует глобальным трендам. Однако успех цифровизации зависит от сбалансированности реформ: технологии должны дополнять, а не заменять гуманитарную суть правосудия. Для этого необходимо развивать нормативную базу, инвестировать в образование юристов и обеспечивать равный доступ к цифровым сервисам. В перспективе сочетание технологий и традиционных правовых ценностей способно сделать российское правосудие более эффективным и справедливым.

Современное информационное общество ставит перед Россией задачу не просто механического внедрения технологий, но формирования новой правовой культуры, где инновации служат инструментом укрепления верховенства права.

Признавая технологический прорыв в развитии судебной системы нашей страны, автор считает, что сформированные условия в сфере судопроизводства в связи с развитием цифровой экономики, уже в настоящее время определяют позитивную динамику развития общественных отношений и создают комфортные условия в сфере оказания правовых услуг населению. Кроме того, особенно ценны последние исследования, посвященные цифровизации судопроизводства, а в частности – электронного доказательства [12. С. 288].

Список литературы

1. Официальный портал Президент РФ. URL: http://kremlin.ru/acts/news/73986 , свободный.

2. Концепции информатизации судов и системы Судебного департамента до 2030 г., утвержденной Постановлением Президиума Совета судей Россий-

ской Федерации от 2 декабря 2019 г. № 785. URL: https://base.garant.ru/402995550/ (дата обращения: 09.09.2025).

3. Федеральный закон от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // Собрание законодательства РФ. 2008. № 52 (ч. 1). Ст. 6217.

4. Концепция информатизации Верховного Суда Российской Федерации (утв. приказом Председателя Верховного Суда РФ от 15.02.2021 № 9-П. URL: http://vsrf.ru по состоянию на 03.03.2021.

5. Официальный сайт ГАС РФ Правосудие // URL: https://sudrf.ru/; Официальный сайт Мой АРБИТР. URL:https://my.arbitr.ru/#index .

6. Паспорт национального проекта "Национальная программа "Цифровая экономика Российской Федерации" (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7.URL: https://digital.gov.ru по состоянию на 09.09.2025.

7. Бурдина Е.В. Цифровизация судебной деятельности: направления, прогнозы и риски // Администратор суда. 2020. № 2. С. 10-14.

8. Васючкова О.А. Цифровая модель вида (внешнего облика): вопросы внедрения и применения в рамках реализации мероприятий комплексного развития территории (КРТ) / В сб.: Сочинские цивилистические чтения. Эволюция цивилистики в современном мире. сборник материалов Международной научно-практической конференции. Сочи-Ростов-на-Дону. 2024. С. 103-114.

9. Завьялова М.П., Сухушин Д.В. Изменения установок гуманитарного образования в условиях становления информационного общества. Открытый междисциплинарный электронный журнал ТГУ «Гуманитарная информатика». URL: http://huminf.tsu.ru/ (дата обращения: 09.09.2025).

10. Кирамов Б.М. Влияние цифровизации на трансформацию мировой экономики // Экономика и менеджмент инновационных технологий. 2025. № 3. URL: https://ekonomika.snauka.ru/2025/06/24750 (дата обращения: 12.09.2025).

11. Новикова В. С. Перспективы развития государственного управления в контексте информационных технологий // Электронный научный журнал «Дневник науки». 2019. № 3. С. 73.

12. 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 347.97/.99

Т. Г. Каракулов,
председатель суда,
Чаинский районный суд Томской области

Сервисы системы межведомственного электронного взаимодействия в суде первой инстанции

Аннотация. В статье предлагаются меры, способствующие обоснованному и своевременному рассмотрению судебных дел с использованием передовых технических достижений для установления юридически значимых обстоятельств. Отмечается важная роль системы межведомственного электронного взаимодействия, функционирующей в судах общей юрисдикции посредством использования программно-технического комплекса обеспечения информационного взаимодействия ГАС «Правосудие» с другими (внешними) информационными системами.

Ключевые слова: рассмотрению судебных дел, суд первойинстанции, информационные технологии, система межведомственного электронного взаимодействия

T. G. Karakulov,
Chairman of the
Chainsky District Court of the Tomsk region

Services of the interdepartmental electronic interaction system in the court of first instance

Abstract. The article suggests measures to facilitate the reasoned and timely consideration of court cases using advanced technical achievements to establish legally significant circumstances. The important role of the interdepartmental electronic interaction system functioning in courts of general jurisdiction through the use of a software and hardware package for ensuring information interaction between GAS "Justice" and other (external) information systems is noted.

Keywords: consideration of court cases, court of first instance, information technology, system of interdepartmental electronic interaction

Введение. Цифровые технологии настолько быстро входят не только в повседневную жизнь, но и в такие специальные сферы, как уголовное судопроизводство, что наука не может оставаться в стороне и отворачиваться от вопросов, которые, на первый взгляд, не имеют какого-то реального практического применения [1. С. 482].

При рассмотрении и разрешении судебных дел суд первой инстанции оперирует различными данными. Большинство из них содержатся в материалах судебных дел: уголовных, гражданских и административных, дел об административных правонарушениях. Однако не всегда имеющихся материалов дела и

доказательств, представленных сторонами и участниками процесса достаточно для принятия решения по делу.

Основная часть. Принимая во внимание необходимость соблюдения не только процессуальных, но и разумных сроков судопроизводства, в определенной части восполнить пробел в установлении юридически значимых обстоятельств по делу возможно путем применения сервисов системы межведомственного электронного взаимодействия.

В судах общей юрисдикции указанная система начала формироваться с 2016 года путем налаживания взаимодействия с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций для информационного обмена судебными постановлениями, касающимися признания информации запрещенной к распространению на территории Российской Федерации.

В конце обозначенного года было заключено Соглашение между указанной Федеральной службой и Судебным департаментом при Верховном Суде Российской Федерации

Федеральным государственным бюджетным учреждением «Информационно-аналитический центр поддержки ГАС «Правосудие» организована доработка программного изделия «Судебное делопроизводство» подсистемы «Судебное делопроизводство и статистика» ГАС «Правосудие», а также разработка сервиса, обеспечивающего передачу на исполнение в единую информационную систему Роскомнадзора судебных решений о признании информации запрещенной к распространению на территории Российской Федерации (или о признании информационных материалов экстремистскими) в форме электронных документов, подписанных усиленными квалифицированными электронными подписями судей, а также сведений о них посредством системы межведомственного электронного взаимодействия.

В 2019 году проведена опытная эксплуатация специального программного обеспечения в соответствии с Регламентом информационного обмена между Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и судебными органами Российской Федерации в рамках первого этапа интеграции единой информационной системы Роскомнадзора 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 обеспечения информационного взаимодействия ГАС «Правосудие» с другими (внешними) информационными системами.

Количество документов, направленных федеральными судами Томской области с использованием указанного программно-технического комплекса, возрастает значительными темпами.

Судом могут быть оперативно запрошены необходимые сведения месте работы и о доходах участников процесса из ФНС, о спорном имуществе – из Росреестра, о возбужденных в отношении участников процесса исполнитель-

ных производствах – из ФССП, а также иные данные, например, из МВД или Социального Фонда России.

Заключение. Изложенное позволяет утверждать, что наряду с этим, цифровые технологии могут эффективно использоваться для развития программно-технического комплекса обеспечения информационного взаимодействия ГАС «Правосудие» в целях полного и достоверного установления судом юридически значимых обстоятельств для разрешения уголовных, гражданских и административных, дел об административных правонарушениях. Имеются дальнейшие перспективы развития уголовного судопроизводства, а именно ведения понятий «электронные доказательства», «электронные данные», предназначенные для слома устаревшей системы документарных «иных документов» [2. С. 289].

Список литературы

1. Спиридонов М.С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481–497. https://doi.org/10.21202/jdtl.2023.20. EDN: acsqxh.

2. 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 347:004

Л.В. Бертовский,
доктор юридических наук, профессор,
Московская Академия Следственного комитета
Российской Федерации,
С. М. Курбатова,
доктор юридических наук, профессор,
Сибирский федеральный университет,
Красноярский государственный аграрный университет

О некоторых рисках использования искусственного интеллекта в системе правосудия: зарубежный опыт

Аннотация. Целью является характеристика рисков использования технологий искусственного интеллекта в судебной системе, опираясь на опыт ряда зарубежных государств. Выделены основные риски применения искусственного интеллекта в судах в контексте технологических и иных факторов. Отмечены позитивные и негативные тенденции дальнейшего внедрения технологий искусственного интеллекта в систему правосудия. Сделан вывод, что использование ИИ в судах может привести как к выгодам, так и к проблемам, что обуславливает необходимость аналитической работы по своевременному выявлению существующих рисков и поиску средств для их устранения или минимизации негативных последствий.

Ключевые слова: правосудие, судебная система, искусственный интеллект, риски, законность, эффективность, безопасность

L.V. Bertovsky,
Doctor of Law, Professor,
Moscow Academy of the Investigative Committee of the RussianFederation,
S. M. Kurbatova,
Doctor of Law, Professor,
Siberian Federal University,
Krasnoyarsk State Agrarian University

On some risks of using artificial intelligence in the justice system: foreign experience

Abstract. The aim is to characterize the risks of using artificial intelligence technologies in the judicial system, based on the experience of a number of foreign countries. The main risks of using artificial intelligence in courts are highlighted in the context of technological and other factors. Positive and negative trends in the further implementation of artificial intelligence technologies in the justice system are noted. It is concluded that the use of AI in courts can lead to both benefits and problems, which necessitates analytical work on the timely identification of existing risks and the search for means to eliminate them or minimize negative consequences.

Keywords: justice, judicial system, artificial intelligence, risks, legality, efficiency, security

Введение. Развитие современных технологий, в том числе искусственного интеллекта (далее – ИИ), происходящее на данном этапе, охватывает все большие сферы общества и государства. Коснулось и системы правосудия. Внедрение искусственного интеллекта в судебную систему, как и в любую другую, направлено на достижение определенного результата. Учитывая специфику отправления правосудия, это: повышение качества судебным процессов и эффективности рассмотрения судами разных категорий дел, содействие обеспечению доступа граждан к судебным ресурсам, юридическим консультациям и представительству, сокращение государственных и частных издержек и др. Системы искусственного интеллекта могут обрабатывать огромные объемы данных и предоставлять анализ, новый контент или решения гораздо быстрее, чем люди. ИИ может обобщать судебные дела или документы гораздо быстрее, чем исследователь-человек. Чат-боты и другие инструменты приема предназначены для того, чтобы помочь людям понять и классифицировать юридические проблемы, а затем предоставить им соответствующую юридическую консультацию по ее решению в судебном порядке или представительство [11, 17]. Искусственный интеллект также может предоставлять альтернативные методы разрешения споров, сокращая количество дел, передаваемых в суд [17]. Если искусственный интеллект интегрирован в слушания с помощью субтитров или перевода в режиме реального времени, это может помочь некоторым пользователям судов легче участвовать в разбирательствах. Искусственный интеллект может даже помочь сторонам, представляющим интересы самих себя, взаимодействовать с судебной системой [15, 19]. И многое другое может искусственный интеллект [2]. Казалось бы, налицо сплошная выгода от внедрения ИИ в систему правосудия. Однако, наряду с плюсами, как и в любой другой деятельности, в процессе использования ИИ в судах имеются и минусы, а точнее разного рода риски, которые необходимо учитывать, чтобы не возникли уже конкретные проблемы.

Основная часть. В ряде стран технологии искусственного интеллекта не просто начали внедряться в судебную систему, но уже и показали результат, причем как положительный, так и отрицательный. Это позволяет проводить анализ деятельности по использованию ИИ в сфере осуществления правосудия, опираясь на имеющийся опыт. Например, в октябре 2024 г. был опубликован отчет Комиссии по правовой реформе штата Виктория Содружества Австралии по использованию искусственного интеллекта в судебной системе, сведения из которого использованы в настоящей работе [4]. В частности, посредством анализа конкретных примеров в австралийских (и не только) судах Комиссией были выделены конкретные риски использования ИИ в судебных процедурах, что подтверждается и другими исследованиями:

– проблемы безопасности и конфиденциальности данных, обрабатываемых технологиями, включая риски передачи третьим лицам, хакерские атаки, технические сбои и др [14];

– непрозрачность технологии искусственного интеллекта относительно алгоритмов принятия решений, по поводу чего высказывают опасения и сами разработчики IT-технологий. Так, в 2023 г. инсайдер компании Google и обозреватель The New York Times Макс Фишер в своей книге «Машина хаоса» по этому поводу написал, что современные компьютерные разработки проходят через такое количество слоев алгоритмов машинного обучения, что человек уже не может заглянуть в код и проследить, почему программа сделала именно такой выбор [10]. Подобное для системы правосудия недопустимо: алгоритм принятия судебных решений должен быть понятен [1], а сами они – соответствовать предъявляемым к ним требованиям, в том числе быть обоснованными и законными [3, 7];

– предвзятость, включая предвзятость как самих данных, так и их результатов. Так, если модель построена с использованием необъективных данных (о неравенстве, дискриминации и пр.) это приведет к необъективным результатам [5], что есть серьезная проблема для судов, где основополагающими принципами являются справедливость, равноправие и отсутствие дискриминации. В судебной практике уже выявлены подобные факты при привлечении ИИ к избранию меры пресечения в виде заключения под стражу, когда представители некоторых рас и национальностей априори воспринимались программой как опасные, а значит, подлежащие изоляции от общества [3];

– неточности и искажения, включая придумывание искусственным интеллектом различных ситуаций. И если первые возникают из-за того, что даже системы, основанные на правилах и алгоритмах, могут давать неточные результаты вследствие ограниченности данных, на которых построена модель, то вторые – это небрежное отношение пользователей к получаемой им информации, когда не перепроверка ими сведений, сгенерированных ИИ, приводит к проигрышу в судебных спорах. Так, в деле Чжан против Чена адвокат подал уведомление о подаче жалобы, содержащее несуществующие юридические данные, которые были выдуманы (‘галлюцинированы’) ChatGPT [20]. Административная ошибка, допущенная предварительно одобренным программным обеспечением для развода, используемым в судах по семейным делам в Англии и Уэльсе привела к тому, что 2235 дел были вновь открыты и переданы на рассмотрение в суд [6, 8]. Ярким примером искажений можно назвать проблему все более распространяющихся дипфейков. Так, фальшивую аудиозапись, на которой родитель угрожает своему ребенку, представили в качестве доказательства в споре об опеке в Соединенном Королевстве [13];

– снижение качества результатов и обесценивание человеческих суждений: системы ИИ предоставляют возможности для повышения эффективности и продуктивности, но могут снизить качество судебных разбирательств, так как более быстрые и дешевые процессы не обязательно приводят к улучшению результатов, а сам искусственный интеллект хоть и может заменить некоторые механистические аспекты работы юриста, но юридические навыки, которые основаны на человечности и этике юриста, ИИ заменить не способен [12];

– проблемы с доступом к правосудию, так как многие граждане недостаточно владеют компьютерными и иными технологиями, да и в принципе далеко

не во всех местностях даже технологически развитых государств есть технические возможности для такого доступа.

Можно говорить о постановке и выделении и других вопросов и проблем относительно использования в судебной системе технологий ИИ. В том числе это неопределенность соответствующей нормативной правовой базы и неслаженность механизма ее реализации; потребности больших финансовых вложений для развитие данной отрасли; необходимость переквалификации работников юстиции на предмет обучения работы с современными высокими технологиями; угроза независимости судебной власти; подрыв доверия общественности к судьям, судебным инстанциям и судебным решениям; и другие [6, 16].

Заключение. Таким образом, использование ИИ в судах может привести к выгодам, рискам и проблемам.

Сложившийся в уголовно-процессуальной науке оптимистичный подход к оценке возможностей применения технологий искусственного интеллекта в уголовном процессе не выдерживает критики [21. С. 490]. Эти риски и выгоды будут различаться в зависимости от типа системы ИИ и способа ее использования. Риски и выгоды будут меняться в зависимости от того, применяется ли система ИИ к сценарию, для которого она была разработана и протестирована, и используется ли она для надлежащих и законных целей [4]. Однако наличие рисков обуславливает необходимость своевременной аналитической работы по выявлению возможных проблем и поиску средств для их устранения или минимизации негативных последствий.

Список литературы

1. Бертовский Л. В. Высокотехнологичное право: современные вызовы // Высокотехнологичное право: современные вызовы: Материалы IV Международной межвузовской научно-практической конференции, Москва-Красноярск, 17–20 февраля 2023 года. Том Часть 1. Красноярск: Красноярский ГАУ, 2023. С. 26-30.

2. Карих К. Г., Сороковиков П. Д. Перспективы и возможности использования искусственного интеллекта в судопроизводстве // Global and Regional Research. 2023. Т. 5, № 3. С. 153-158.

3. Andrew D Selbst and Solon Barocas The Intuitive Appeal of Explainable Machines // Fordham Law Review. 2018. 87.

4. Artificial Intelligence in Victoria's Courts and Tribunals: Consultation Paper. 2024. October, 17. URL: https://www.lawreform.vic.gov.au/publication/artificial-intelligence-in-victorias-courts-and-tribunals-consultation-paper/ (дата обращения: 09.08.2025).

5. Australian Human Rights Commission, Human Rights and Technology (Final Report). 2021. May, 27. URL: https://humanrights.gov.au/our-work/technology-and-human-rights/projects/final-report-human-rights-and-technology (дата обращения: 09.08.2025).

6. Bell A. Truth Decay and Its Implications: An Australian Perspective. Speech, 4th Judicial Roundtable. Durham University. 2024. April, 23. URL:

https://supremecourt.nsw.gov.au/supreme-court-home/about-us/speeches/chief-justice.html (дата обращения: 09.08.2025).

7. Burrell J. How the Machine “Thinks”: Understanding Opacity in Machine Learning Algorithms // Big Data & Society. 2016. 3(1).

8. Contini F. Artificial Intelligence and the Transformation of Humans // Law and Technology Interactions in Judicial Proceedings. 2020. 2(1).

9. Felicity Bell et al. AI Decision-Making and the Courts: A Guide for Judges, Tribunal Members and Court Administrators. Report, Australasian Institute of Judicial Administration. 2023. December. URL: ai-decision-making-and-the-courts_report_v5-2022-06-20-1lzkls.pdf (дата обращения: 09.08.2025).

10. Fisher M. The chaos machine: The Inside Story of How Social Media Rewired Our Minds and Our World. Little, Brown & Company. URL: https://habr.com/ru/news/687506/ (дата обращения: 09.08.2025).

11. Law Council of Australia. The Justice Project. Final Report. 2018, August. URL: https://lawcouncil.au/files/web-pdf/Justice%20Project/Final%20Report/Justice%20Project%20_%20Final%20Report%20in%20full.pdf. (дата обращения: 09.08.2025).

12. Legg M. and Bell F. Artificial Intelligence and the Legal Profession: Becoming the AI-Enhanced Lawyer // University of Tasmania Law Review 2019. 38(2).

13. McPeak A. The Threat of Deepfakes in Litigation: Raising the Authentication Bar to Combat Falsehood // Vanderbilt Journal of Entertainment & Technology Law 2021. 23(2).

14. Office of the Victorian Information Commissioner, Artificial Intelligence – Understanding Privacy Obligations. Report 2021. April. URL: https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-understanding-privacy-obligations/ (дата обращения: 09.08.2025).

15. Schmitz A. and Zeleznikow J. Intelligent Legal Tech to Empower Self-Represented Litigants // Science and Technology Law Review. 2022. 23(1).

16. Sourdin T. Judges, Technology and Artificial Intelligence: The Artificial Judge. Edward Elgar Publishing. 2021.

17. Susskind R. Online Courts and the Future of Justice. Oxford University Press. 2019.

18. The Law Society of England and Wales, Technology, Access to Justice and the Rule of Law. Report, The Law Society of England and Wales. 2019. September.

19. Tulk N., Gorst Ch. and Shanks L. The Legal Access Challenge: Closing the Legal Gap through Technology Innovation. Report, Solicitors Regulation Authority. 2020. June.

20. Zhang v Chen [2024] BCSC 285 URL: https://obiter-dicta.ca/2024/04/01/zheng-v-chen-a-warning-against-the-use-of-ai-in-family-law/ (дата обращения: 09.08.2025).

21. Спиридонов М.С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481–497. https://doi.org/10.21202/jdtl.2023.20. EDN: acsqxh.

УДК 004/34.06

П. Н. Мазуренко,
кандидат юридических наук, доцент,
Казанский институт (филиал) ВГУЮ (РПА Минюста России)

Применение цифровых технологий в адвокатской деятельности

Аннотация. В статье рассмотрено применение цифровых технологий в адвокатской деятельности. Рассмотрены как положительные, так и отрицательные аспекты их использования. Рассмотрено создание цифрового личного бренда адвоката, использование Государственной автоматизированной системы «Правосудие», электронного документооборота, обучение и повышение квалификации адвоката. Статья может быть использована в адвокатской практике и в целях дальнейшего совершенствования нормативного регулирования.

Ключевые слова: адвокатская деятельность, цифровизация, цифровой личный бренд адвоката, повышение квалификации, адвокат, цифровые технологии, цифровая трансформация

P.N. Mazurenko,
Candidate of Legal Sciences, Senior Lecturer,
Kazan Institute (branch) VSUYU (RPA of the Ministry of Justice of Russia

Application of digital technologies in advocacy

Abstract. The article discusses the use of digital technologies in advocacy. Both positive and negative aspects of their use are considered. The creation of a digital personal brand of a lawyer, the use of the State Automated System "Justice," electronic document management, training and advanced training of a lawyer were considered. The article can be used in law practice and in order to further improve regulatory regulation.

Keywords: advocacy, digitalization, digital personal brand of a lawyer, advanced training, , lawyer, digital technologies, digital transformation

Введение. Цифровизация может найти применение во многих областях науки, включая, в частности, гуманитарные и общественные дисциплины [2. С. 237]. Внедрение цифровизации в адвокатскую деятельность обоснованна неумолимым временем. В то же время в этом неотвратимом процессе есть ряд как положительных моментов, так и определенные отрицательные аспекты.

Основная часть. Начнем с положительной составляющей. Во-первых, это возможность создания личного цифрового бренда адвоката с использованием социальных сетей, сайтов, электронной подписи и других онлайн-инструментов для привлечения доверителей, общения с коллегами и широким кругом населения. Адвокат должен уметь, не нарушая требований по этике и

стандартам адвокатской деятельности, информировать общественность о своей деятельности, в том числе и оказываемой в рамках бесплатной юридической помощи, волонтерской деятельности, спортивных и творческих достижениях. Многие адвокаты активно участвуют в помощи бойцам СВО, пишут книги, стихи, участвуют в спортивных соревнованиях. И самый лучший способ довести информацию об этом – это комментарии, использование средств массовой информации, социальных сетей, создание личных каналов, страничек в периодических изданиях, что невозможно без информатизации. Кроме того, изучая открытые источники в социальных сетях и средствах массовой информации, адвокат может получить большой массив информации о своих оппонентах и подготовиться к процессу. В то же время сам он не должен выкладывать информацию, которая может причинить вред ему самому или его доверителям, а также нарушить адвокатскую тайну и этические критерии, и стандарты адвокатской деятельности.

Второе – это возможность быстро находить нужную информацию в электронных базах данных, включая законодательство, судебную практику, научные публикации и образцы документов на заданную тему. Адвокаты уже достаточно давно используют компьютерные справочно-правовые системы «Гарант» и «КонсультантПлюс». Законодательство в России меняется чрезвычайно быстро и сейчас без использования справочных систем адвокатская деятельность практически невозможна. При составлении любого документа, будь то жалоба или иск, адвокат обязательно обращается к справочным системам проверяя текс на соответствие современному состоянию нормативных актов, что позволяет исключить ссылки на устаревшее законодательство и не актуальную правоприменительную практику.

Третье направление – автоматизация делопроизводства и офисной деятельности, в том числе в сфере распределения уголовных дел по назначению в порядке ч. 2 ст. 50 УПК РФ посредством Комплексной информационной системы адвокатуры России (КИС АР). Данная система должна интегрировать с информационными системами судов, правоохранительных органов и других структур с целью перехода адвокатуры на электронный документооборот с государственными информационными системами (Минюст России, ФСИН России, ГАС «Правосудие», ФНС России и другими), при этом сохраняя информационную стабильность и независимость адвокатуры.

В адвокатской деятельности активно используются информационные технологии, упрощающие хранение, поиск и обмен документами, что также снижает затраты на делопроизводство. При этом существенно ускоряется процесс передачи документов доверителям, коллегам и получения информации из различных источников. Так, используя видеоконференции можно провести консультации или совещания с доверителями или специалистами находящихся в других городах и даже странах. Так, в моей практике проводились консультации со специалистами, находящимися в г. Москве и доверителями, постоянно проживающими в Израиле, Германии и других странах. В процессе делопроизводства возможно использование электронных подписей, которые упрощают процесс подписания документов и позволяют многие вопросы решать удаленно.

Электронная подпись позволяет более эффективно использовать систему «Госуслуги» и ГАС «Правосудие». Через портал Госуслуги можно подавать иски, обмениваться отзывами на них, направлять жалобы и получать судебные акты. В рамках системы ГАС «Правосудие» имеется возможность создания личного кабинета, который позволяет получать копии различных судебных решений и других документов в электронном виде. Неплохо работает система извещения путем СМС участников процесса.

Четвертое направление – повышение квалификации и обучение адвокатов. В наличие большое количество онлайн-курсов и вебинаров по подготовке к сдаче экзамена на статус адвоката, повышения квалификации по различным направлениям и специализации позволяют юристам существенно совершенствовать свои знания и навыки. Так вебинары, проводимые Федеральной адвокатской палатой, засчитываются как повышение квалификации с выдачей соответствующего сертификата.

В целом цифровые технологии значительно улучшают эффективность и качество работы адвокатов, позволяя им предоставлять более качественные юридические услуги.

В то же время, учитывая творческий характер адвокатской деятельности надо учитывать и отрицательные аспекты процесса информатизации.

Так сбой в работе ГАС «Правосудие», который произошел в октябре 2024 года, показал уязвимость работы подобных систем. Все уже привыкли получать актуальную информацию на официальных сайтах судов. В результате в работе адвокатов возникли существенные сложности.

Кроме того, при внедрении информационных технологий необходимо учитывать, то, что адвокатская деятельность достаточно консервативна. Консервативность отражается и в законодательстве, и в этических критериях адвокатской деятельности и, даже, в требованиях к внешнему облику адвоката. Помниться, что лет 30 назад многие юристы заявляли о том, что цифровая фотография в криминалистике не приживется, так как отсутствует негатив, который можно приложить к протоколу. Сейчас это воспринимается как забавная шутка. Думается, что многое из того, что сейчас кажется почти фантастикой через несколько лет станет обыденной практикой адвокатов России. Надо учесть и то, что в профессию адвоката люди приходят уже имея солидный профессиональный опыт и возраст. Так доля адвокатов в возрасте старше 60 лет в последние годы увеличилась с 14,9 до 17 % [2]. Очевидно, что взрослым людям сложнее осваивать новые технологии и включаться в процесс цифровизации. При этом очевидно, что невозможно оцифровать жизненный и профессиональный опыт, адвокатскую интуицию, судебное усмотрение и использование тактических и психологических приемов в адвокатской деятельности.

Думается, что сами по себе цифровые технологии не угрожают профессии адвоката. Нам кажется, что в ближайшее время заменить профессиональную творческую деятельность адвоката искусственным интеллектом не получиться. Искусственный интеллект будет по-прежнему полезен только в целях повышение эффективности научной организации труда в части формализованных функции и сбора информации. По крайне мере, я на это надеюсь.

Для адвокатского сообщества может представлять угрозу только формализация и волюнтаристский подход к проблемам внедрения искусственного интеллекта и цифровизации, а также адаптации правовой системы к новым реалиям.

Заключение. Действующее законодательство и адвокатская практика в части цифровизации адвокатской деятельности пока еще далека от совершенства. Пока еще не решены многие как правовые, так и чисто технические вопросы, возникающих в ходе применения цифровых технологий. В данном случае необходимо использовать имеющийся опыт других стран, к примеру Сингапура, Казахстана по внедрению электронного уголовного и административного делопроизводства, которые существенно продвинулись в решении данных вопросов.

Список литературы

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

2. Сколько зарабатывают адвокаты. И в каком регионе их больше всего. Источник: экспертная группа «Вета». URL: https://t-j.ru/advocate-stat/?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 06.09.2025).

УДК 343

А. А. Петрикина,
кандидат юридических наук, доцент,
Северо-Кавказский филиал
Российского государственного университета правосудия
имени В. М. Лебедева»

О возможности применения технологии искусственного интеллекта при избрании в качестве меры пресечения заключения под стражу

Аннотация. Особенности использования норм уголовно-процессуального законодательства, посвященных мерам пресечения тревожат уже несколько десятков лет научную общественность и не перестают быть актуальными, особенно в свете применения технологии искусственного интеллекта. Изменения социально-политического и экономического характера определили цель исследования, которая представляет собой изучение и анализ проблем, возникающих при реализации института заключения под стражу в условиях перманентного технологического развития. В качестве задач определены: изучение проблем избрания в качестве меры пресечения заключения под стражу и использованием технологии искусственного интеллекта, выявление роли прокуратуры и суда в данном процессе; поиск проблем правового регулирования и путей их решения. В результате исследования решены сложные вопросы, касающиеся реализации правовых норм о заключении под стражу с использованием новых технологий.

Ключевые слова: искусственный интеллект, заключение под стражу, мера пресечения, уголовный процесс, прокурор, защитник, суд

A. A. Petrikina
Candidate of Law, Senior Lecturer,
North Caucasus Branch,
Russian State University of Justice
named after V. M. Lebedev

On the possibility of using artificial intelligence technology when choosing detention as a preventive measure

Abstract. The peculiarities of the use of the norms of criminal procedural legislation devoted to preventive measures have been worrying the scientific community for several decades and do not cease to be relevant, especially in light of the use of artificial intelligence technology. Changes in socio-political and economic nature determined the purpose of the study, which is the study and analysis of the problems arising in the implementation of the institution of detention in the context of permanent technological development. The following tasks are defined: studying the problems of choosing detention as a preventive measure and using artificial intelligence

technology, identifying the role of the prosecutor's office and the court in this process; searching for problems of legal regulation and ways to solve them. As a result of the study, complex issues related to the implementation of legal norms on detention using new technologies were resolved.

Key words: artificial intelligence, detention, preventive measure, criminal proceedings, prosecutor, defense attorney, court

Введение. Под технологией искусственного интеллекта в уголовном судопроизводстве следует понимать автоматизированные процессы, позволяющие оптимизировать раскрытие, расследование и последующее рассмотрение уголовных дел в суде на основе заданных человеком алгоритмов и прочих данных.

Федеральным законом от 28.02.2025 № 13-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» в статью 108 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) введены поправки, предусматривающие ограничения применения меры пресечения в виде заключения под стражу. Сегодня она применяется в отношении лиц, подозреваемых или обвиняемых в совершении преступлений средней тяжести насильственного характера, тяжких или особо тяжких преступлений.

Заключение под стражу подозреваемого (обвиняемого) применяется только при наличии определенных условий. Искусственный интеллект способен проверить, имеют ли они место в конкретном уголовном деле (по учетам МВД России, имеется ли регистрация в качестве субъекта хозяйственной деятельности для предпринимателей и постановка на налоговый учет в ИФНС, были ли нарушены ранее избранные меры пресечения). Речь не идет о принятии конкретного уголовно-процессуального решения при их наличии. Для этого уголовно-процессуальным законом четко обозначены лица, обладающие специальными полномочиями.

Искусственный интеллект также может прийти на помощь, когда быстро надо найти информацию в органах, ведущих записи актов гражданского состояния и их архивы, опеки и попечительства, социального обеспечения населения.

Фактические данные, которые ложатся в основу положительного решения о заключении лица под стражу, должны быть в обязательном порядке исследованы в судебном заседании [1].

В большинстве случаев закон не содержит предписаний о том, что в каких-то случаях меры пресечения должны избираться в обязательном порядке, по каждому уголовному делу учитывается совокупность обстоятельств, о которых упоминается в ст. 97 УПК РФ [7].

При избрании данной меры пресечения, пожалуй, самой суровой, институт адвокатуры позволяет гарантировать неприкосновенность личности, повышает уровень доверия граждан к правоохранительным органам и судебной власти. Именно оказание профессиональной помощи может помочь доказать невиновность лица, и не допустить нарушение его конституционных прав. Вопрос о правовом статусе защитника и его процессуальном положении всегда являлся одним из более дискуссионных в науке уголовного процесса. Данный фактор также обусловлен тем, что посредством оказания профессиональной защиты

обеспечивается принцип состязательности, равноправия сторон, достигается соблюдение прав и интересов лица.

Стоит отметить, что правовой статус защитника в настоящее время приобретает новую окраску и детализируется особенно с учетом технологии искусственного интеллекта. Одним из ключевых вопрос является вопрос о степени профессионализма лица, осуществляющего защиту. Искусственный интеллект поможет быстро определить имеет ли лицо юридическое образование, обладает ли статусом адвоката в установленном законом порядке.

Содержание под стражей только в особо исключительных случаях может длиться более 12 месяцев (ч. 3 ст. 109 УПК РФ), однако в практической деятельности эти сроки нередко нарушаются [2. С. 110]. Здесь также можно использовать возможности искусственного интеллекта, который будет вести подсчет срока данной меры пресечения.

Следует согласится с мнением И. М. Хапаева о том, что: «Сроки содержания под стражей лиц, обвиняемых в совершении тяжких и особо тяжких преступлений, до суда по УПК РФ являются неоправданно длительными, обусловливающими частые нарушения требования разумности, и противоречат международным стандартам уголовного судопроизводства. Предельный срок по данным категориям дел нужно сократить до девяти месяцев» [9. С. 149].

Н. В. Буланова полагает, что «прокурор, выявив отсутствие основания для задержания или нарушение его порядка (в том числе истечение сроков при отсутствии судебного решения о помещении под стражу), может вынести процессуальное решение о незамедлительном освобождении лица для соблюдения его конституционных прав» [3. С. 110-112]. Аналогичной позиции придерживаются С. П. Щерба и Д. И. Ережипалиев [10. С. 108].

Прокурор может своим постановлением освободить лицо из-под стражи при выявлении факта невыполнения обязанности должностного лица органа расследования отменить или изменить меру пресечения при наличии к тому оснований, включая случаи превышения предельных сроков или прекращения уголовного дела (п. 8 ч. 1 ст. 212 УПК РФ) [5. С. 154]. При этом прокурор в таких случаях самостоятельно освобождает обвиняемого своим решением, а не обязывает это сделать должностных лиц, осуществляющих предварительное расследование [4. С. 50-52].

Также необходимость освободить лицо может возникнуть при переквалификации на менее тяжкое или просто иное деяние, которое подпадает под установленные законом ограничения применения заключения под стражу (ч. 1.1, 2 ст. 108 УПК РФ). Технически отследить этот момент также может искусственный интеллект.

При принудительном помещении лица в медицинский или психиатрический стационар, у прокурора имеется аналогичная возможность освободить его, если выяснится незаконный характер его там пребывания. И здесь искусственный интеллект может помочь [8].

Заключение. Органы предварительного расследования нередко ходатайствуют об избрании меры пресечения в виде заключения под стражу только лишь

для подстраховки. Однако данные субъекты, а также прокурор и суд, обладая широкими полномочиями, должны предотвращать случаи необоснованного ограничения прав подследственных на свободу и личную неприкосновенность и в этом во многом может помочь технология искусственного интеллекта [6].

При этом необходимо:

– в целях оптимизации технической работы судов и правоохранительных органов допустить на законодательном уровне возможность использования искусственного интеллекта;

– ограничить внедрение данной технологии путем запрета ее применения при окончательном принятии уголовно-процессуального решения,

– предусмотреть проверку при возникновении сомнений, полученных с помощью этой технологии сведений по уголовному делу специалистом.

Список литературы

1. Апелляционное постановление № 22-5454/2020 от 27 августа 2020 г. по делу № 1-133/2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/UsRaJkADoxlV (дата обращения: 09.08.2025).

2. Ахмед К. С. А. Гарантии прав личности в досудебном производстве по уголовно-процессуальному законодательству России и Ирака: дисс. … канд. юрид. наук. Ростов-на-Дону, 2017. 210 с.

3. Буланова Н. В. Прокурорский надзор за соблюдением прав участников уголовного судопроизводства: состояние, проблемы, перспективы // Уголовное право. 2011. № 2. С. 107-113.

4. Каретников А. С., Каретников С. А. Сущность полномочий прокурора по надзору за предварительным следствием: прошлое и настоящее // Российская юстиция. 2015. № 5. С. 49-52.

5. Коломеец Е. В. Использование прокурором средств реагирования в досудебном производстве: диссертация … канд юрид. наук. М., 2019. 258 с.

6. Обзор практики рассмотрения судами ходатайств об избрании меры пресечения в виде заключения под стражу и о продлении срока содержания под стражей (утв. Президиумом Верховного Суда РФ 18.01.2017) // Бюллетень Верховного Суда Российской Федерации: официальное издание. 2017. № 9. С. 34.

7. Постановление Пленума Верховного Суда РФ от 19.12.2013 № 41 «О практике применения судами законодательства о мерах пресечения в виде заключения под стражу, домашнего ареста, залога и запрета определенных действий» (ред. от 11.06.2020) // Бюллетень Верховного Суда РФ. 2014. № 2.

8. Приказ Генпрокуратуры России от 17.09.2021 № 544 «Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия» (ред. от 22.02.2023) // Законность. 2021. № 2.

9. Хапаев И. М. Заключение под стражу как мера пресечения в российском уголовном судопроизводстве: монография. М.: Юрлитинформ, 2013. 197 с.

10. Щерба С. П., Ережипалиев Д. И. Прокурор в досудебном производстве по уголовным делам: функции, правовой статус, полномочия: монография. М.: Юрлитинформ, 2015. 165 с.

УДК 342.565

И. Ю. Шумейко,
кандидат юридических наук, доцент,
Ростовский государственный экономический университет

Цифровая трансформация системы правосудия Российской Федерации

Аннотация. Статья посвящена актуальным вопросам внедрения цифровых технологий в систему российского правосудия. Предметом исследования являются этапы цифровой трансформации правосудия в России, выделяющиеся в ходе анализа. Объектом исследования выступают положительные результаты внедрения цифровых технологий в судебную систему, включая правовые аспекты, нуждающиеся в оперативном решении. Анализ затрагивает последовательность технологического развития судопроизводства, существующие препятствия модернизации и будущие направления совершенствования российской системы электронного правосудия. Результаты демонстрируют потребность нормативного закрепления применения инновационных решений в работе судов, раскрывая потенциал автоматизированных процессов для самостоятельного выполнения определенных задач.

Ключевые слова: информатизация, цифровизация, цифровое правосудие, электронное правосудие, интеграция, трансформация правосудия, судопроизводство, эффективность правосудия, информационные технологии в судебной деятельности, искусственный интеллект

I. Y. Shumeyko,
Rostov State University of Economics (RINH),
Candidate of Law, Associate Professor

Digital transformation of the justice system of the Russian Federation

Abstract. The article is devoted to current issues of introducing digital technologies into the Russian justice system. The subject of the study is the stages of digital transformation of justice in Russia, highlighted in the course of the analysis. The object of the study is the positive results of introducing digital technologies into the judicial system, including legal aspects that require prompt resolution. The analysis touches upon the sequence of technological development of legal proceedings, existing obstacles to modernization and future directions for improving the Russian e-justice system. The results demonstrate the need for regulatory consolidation of the use of innovative solutions in the work of courts, revealing the potential of automated processes for the independent performance of certain tasks.

Keywords: informatization, digitalization, digital justice, electronic justice, integration, transformation of justice, legal proceedings, efficiency of justice, information technologies in judicial activity, artificial intelligence

Введение. Цифровая трансформация судебной системы Российской Федерации кардинально видоизменяет устоявшиеся механизмы отправления правосудия, создавая принципиально новые форматы юридической работы. Растущие запросы населения к оперативности рассмотрения дел, результативности судопроизводства и доступности правовой информации стимулируют масштабное внедрение передовых цифровых инструментов в судебную систему. Фундаментальные изменения процессуального взаимодействия между участниками судопроизводства требуют всестороннего научного анализа текущих преобразований.

Научная значимость представленного исследования определяется комплексным изучением процессов преобразования судебной системы в цифровом пространстве, включая определение основных векторов развития и фундаментальных изменений в механизмах отправления правосудия. Полученные результаты способствуют формированию целостного представления о современном состоянии судопроизводства и разработке мер по совершенствованию его цифровой составляющей.

Методологическую основу работы составили системный подход к изучению информации и ее последующий синтез, позволившие провести углубленную оценку достижений и сложностей при внедрении современных технологий в судебную деятельность. Ключевой акцент сделан на изучении правовых аспектов, связанных с недостаточным нормативным регулированием процессов цифровизации, создающим определенные сложности в правоприменительной деятельности.

Комплексное изучение процесса цифровой трансформации судебной системы Российской Федерации позволило выявить ключевые этапы модернизации и актуальные сложности внедрения современных технологий в работу судебных органов. Анализ практического применения указывают на значительный рост продуктивности судебных процессов благодаря оптимизации документального взаимодействия и расширению каналов связи с гражданами, при сохранении существующих законодательных барьеров и технических недоработок, замедляющих становление цифрового судопроизводства.

Выводы исследования подчеркивают необходимость создания устойчивой правовой и технологической основы для эффективного функционирования цифрового правосудия. Первостепенное значение приобретает формирование нормативной базы, регулирующей применение передовых технологий при осуществлении судопроизводства, а также разработка комплексных мер по обеспечению законных интересов населения в условиях масштабной цифровизации. Проведенный анализ способствует глубокому осмыслению преобразований судебной системы и выработке конкретных предложений по совершенствованию механизмов отправления правосудия.

Основная часть. Цифровизация правосудия, или цифровая трансформация, представляет собой многогранный процесс, требующий не только правовых и организационных изменений, но и внедрения современных технологий в судебную систему, при этом строго соблюдая конституционные принципы. Стоит отметить, что до сих пор нет единого понимания того, что именно подразу-

мевается под электронным или цифровым правосудием, как в российской, так и в зарубежной юридической науке. Ключевым моментом в этой дискуссии является то, что понятия «электронное правосудие» и «цифровое правосудие» до сих пор не имеют единого, юридически закрепленного определения. В результате, вокруг них сложились разные интерпретации, что порождает неоднозначность в понимании их сути. Похоже, что эти термины могут быть взаимозаменяемыми, но тем не менее мы считаем, что каждый из этих терминов отражает самостоятельный аспект и, соответственно, отдельную стадию трансформации правосудия.

Процесс цифровой трансформации правосудия, подобно любому иному преобразованию, характеризуется последовательной чередой этапов, каждый из которых призван решать конкретные задачи, вытекающие из актуальных вызовов, стоящих перед судебной системой. Итак, в России можно выделить следующие ключевые периоды, составляющие этапы этой трансформации:

– начальным этапом цифровой модернизации деятельности судов стало внедрение информационных технологий (компьютеризация) в период с 2002 по 2004 год;

– следующим шагом в цифровой трансформации судостроения стала автоматизация работы судов, которая охватила период с 2004 по 2012 год;

– с 2012 по 2021 год развернулась третья волна цифровой трансформации, которая ознаменовалась внедрением ключевых компонентов электронного правосудия;

– в 2021 году и по настоящее время активно реализуется четвертый этап цифровой трансформации, который характеризуется внедрением принципов цифрового правосудия.

Итак рассмотрим подробно первый из ключевых шагов в цифровизации российской судебной системы – информатизация судов. Это означает оснащение судов новейшими компьютерными технологиями, создание для судей, помощников судей и сотрудников аппаратов судов автоматизированных рабочих мест, а также организация локальных вычислительных сетей с доступом к централизованным правовым и другим информационным базам данных [3].

Эволюция цифровой трансформации правосудия неизбежно привела к автоматизации судебных процессов, для чего необходима единая информационно-коммуникационная система. Однако, внедрение автоматизации в арбитражных судах и судах общей юрисдикции шло по разным, независимым друг от друга путям. Внедрение автоматизированных систем в российское судопроизводство ознаменовалось созданием двух ключевых платформ: Единой автоматизированной информационно-коммуникационной системы арбитражных судов (далее – ЕАИКС АС РФ) и Государственной автоматизированной системы «Правосудие» для судов общей юрисдикции (далее – ГАС «Правосудие»).

Программой развития судебной системы России на период с 2007 по 2012 год [2] были выявлены две ключевые проблемы: затяжные судебные процессы, которые приводили к неэффективной защите прав граждан, и недостаточная прозрачность судебной системы. Отсутствие четкого разъяснения мотивов судебных решений и механизмов обеспечения открытости правосудия со-

здавало у граждан ощущение недоверия к судам, что в итоге понижало уровень доверия к судебной системе в целом.

Повышение прозрачности правосудия и укрепление доверия граждан к судебной системе стали приоритетными задачами, для решения которых был принят Федеральный закон от 22.12.2008 № 262-ФЗ [1]. Закон, который начал действовать с 1 июля 2010 года, детально прописывает механизмы предоставления информации о работе судов в разных форматах. Важно подчеркнуть, что этот закон не только возложил на судебные органы обязанность информировать различных субъектов, включая граждан, организации, общественные объединения, государственные и муниципальные органы, но и создал систему мер, гарантирующих и защищающих конституционное право на информацию. Со вступлением в силу Федерального закона от 22 декабря 2008 г. № 262 официальные веб-ресурсы судов, функционирующие в интернете, получили существенное значение и стали ключевыми информационными площадками. Конечно, веб-сайты судов существовали до вступления в силу Федерального закона от 22.12.2008 № 262, тем не менее законодательное закрепление обязательств по актуализации и публикации судебной информации значительно продвинуло развитие правовой системы, обеспечивая реализацию конституционных прав граждан на доступ к правосудию и формируя единое информационное пространство судебной системы с современной электронной инфраструктурой.

Цифровая трансформация правовой системы получила мощный импульс с развитием электронного правосудия. Однако, как отмечалось ранее, в российском законодательстве до сих пор отсутствует четкое определение термина «электронное правосудие», что приводит к разногласиям в юридической среде по поводу его точного смысла.

Романенкова С.В. определяет электронное правосудие (в широком понимании) как комплекс автоматизированных информационных систем, предоставляющих возможности для размещения судебных решений, ведения цифровых дел и обеспечения доступа участников процесса к документам, входящим в состав электронного дела [14. С. 27]. Ю.А. Жданова считает, что электронное правосудие подразумевает не только возможность для суда и участников процесса осуществлять свои законные права и обязанности в цифровом формате, но и включает в себя целый комплекс автоматизированных информационных систем, предназначенных для публикации судебных решений, ведения электронных дел и предоставления сторонам доступа к материалам этих дел [10. С. 80]. По мнению Ф.Р. Гаджиева и Д.А. Панкратова, определение электронного правосудия должно быть более конкретным и звучать так: «электронное правосудие – это использование судьями, сторонами процесса и другими заинтересованными субъектами информационных инструментов для улучшения работы судебной системы и повышения качества правосудия» [9. С. 15].

Начало нового этапа цифровизации правосудия было положено пандемией COVID-19. В 2020 году, когда мир столкнулся с беспрецедентными ограничениями, вызванными пандемией, традиционные способы обращения в суд и участия в судебных процессах оказались фактически невозможными. Это создало серьезные проблемы для реализации права на судебную защиту несмотря

на то, что это право является основополагающим и не подлежит каким-либо ограничениям согласно конституционным нормам. Введение самоизоляции, ограничивающей передвижение граждан за исключением особых ситуаций, существенно осложнило реализацию конституционных прав. В ответ на это, Верховный Суд РФ и Совет судей РФ совместно издали постановления, где представлены рекомендации по организации работы судов и порядку подачи судебных документов, предлагая использовать почтовые или электронные каналы связи [4,5].

Официальные данные Верховного Суда РФ свидетельствуют о высокой популярности электронных ресурсов судебной системы в период действия ограничительных мер, связанных с пандемией коронавируса [13]. Российская судебная система, благодаря своей готовности к внедрению электронных технологий, успешно справилась с беспрецедентными вызовами, возникшими в связи с пандемией. В результате ограничительные меры ускорили развитие электронного правосудия в стране. Соглашаясь с В.В. Момотовым, можно утверждать, что текущая обстановка требовала не просто адаптации к новым реалиям, а создания принципиально новых моделей правосудия. Только они смогут гарантировать доступность, прозрачность и эффективность правосудия, а также защиту прав и свобод граждан, независимо от негативных внешних обстоятельств [15].

Эволюция цифровизации правовой системы привела к появлению и развитию нового этапа – «цифрового правосудия». Определение термина «цифровое правосудие», как и аналогичного ему «электронного правосудия», пока не установлено законодательно. Юристы не пришли к единому мнению относительно точного определения этих понятий и их взаимосвязи. Мы согласны с В.В. Момотовым, который считает, что «цифровое правосудие» подразумевает смещение акцента на цифровые коммуникации, в то время как «электронное правосудие» фокусируется на использовании информационно-коммуникационных технологий судами для разрешения споров [8]. Эволюция правосудия от «электронного» к «цифровому» не только подчеркивает важность электронных документов, но и акцентирует внимание на ключевой роли цифровых доказательств, дистанционных идентификационных процедур и внедрения передовых технологий, таких как искусственный интеллект, в решении как процессуальных, так и общих задач, стоящих перед судами.

Цифровое правосудие, рассматриваемое как логичное продолжение электронного правосудия, пока только начинает формироваться в России. На сегодняшний день в судебной практике применяются лишь отдельные его составляющие, среди которых наиболее заметным является использование искусственного интеллекта, внедрение которого в правовую сферу страны началось сравнительно недавно – весной 2021 года. Использование искусственного интеллекта в судопроизводстве стартовало с задачи автоматизации работы с документами и проверки реквизитов в рамках приказного производства по налоговым долгам в Белгородской области [6]. В 2025 году на Сахалине планируется внедрение ИИ для ведения протоколов судебных заседаний, как было заявлено Министерством цифрового развития региона [7]. В обоих рассматриваемых

сценариях искусственный интеллект выступает инструментом для оптимизации деятельности сотрудников судебного аппарата.

На пленарном заседании Совета судей РФ в мае 2025 года председатель Совета судей РФ Виктор Момотов подчеркнул, что будущее российского правосудия неразрывно связано с переходом на цифровые технологии и использованием искусственного интеллекта [17].

Говоря о текущем этапе развития электронного правосудия в стране, можно отметить, что в нынешнем году Совет судей России берет на себя амбициозную роль главного инициатора изменений в судебной системе. В его активе – ряд законопроектов, направленных на улучшение социальной защиты судей, ускорение цифровизации судопроизводства, реформирование мировой юстиции и снижение судебной нагрузки. В отчетный период комиссия, занимающаяся цифровизацией судопроизводства, разработала проект концепции, направленной на цифровую трансформацию гражданского процесса и судебной деятельности. Этот проект является ключевым этапом в интеграции информационных технологий в судебную систему. Одним из главных направлений концепции является плавный переход к функционированию «электронных судов».

В.В. Момотов высказал мнение, что к 2030 году судопроизводство должно стать полностью цифровым, охватывая все этапы, начиная с подачи заявления и заканчивая получением судебных решений [11]. Для реализации этой концепции необходимо будет пересмотреть действующие процессуальные кодексы, утвердив электронную форму судебных документов, отказаться от традиционного протоколирования в пользу аудио- и видеозаписей, а также создать единую систему электронного документооборота между судами различных инстанций. По информации Судебного департамента в течение 11 месяцев 2023 года департамент зафиксировал подачу порядка 5,5 миллионов документов в электронном формате. Основная часть, составляющая 4,7 миллиона, была направлена в суды общей юрисдикции через платформу «Электронное правосудие», а около 800 тысяч документов – в арбитражные суды, используя сервис «Мой арбитр» [16]. Хотя и невозможно привести достоверную статистику за 2024 год, поскольку с 7 октября 2024 года из-за хакерской атаки был приостановлен доступ к сервисам ГАС «Правосудие», в том числе к модулю «Электронное правосудие», приведенная в пример активность пользователей в 2023 году, свидетельствует о растущей популярности цифровых инструментов, особенно в населенных пунктах, расположенных далеко от крупных городов.

В.В. Момотов считает, что внедрение искусственного интеллекта поможет уменьшить нагрузку на судей и судебные органы. Для реализации этой идеи в апреле 2025 года была сформирована группа, которая займется изучением и масштабированием уже существующих успешных примеров применения ИИ в судебной системе. Опыт внедрения искусственного интеллекта в судопроизводство показал его широкое применение: 35% судов уже используют ИИ. Среди примеров можно назвать Москву, Подмосковье, Башкортостан и Татарстан, где ИИ применяется для автоматизации рутинных задач, таких как распознавание речи и ведение протоколов.

Главная сложность заключается в отсутствии единой информационной платформы. Судебная система опирается на разнородные и устаревшие системы: ГАС «Правосудие» не подлежит модернизации, арбитражные суды функционируют в изолированной среде, а мировые судьи в 13 регионах прибегают к сторонним программам. Такая фрагментация приводит к лишним расходам и снижает эффективность работы. Для решения этих проблем требуется внедрение новой автоматизированной системы, которая объединит все судебные структуры в единое целое.

Отчет Счетной палаты (далее – СП) выявил, что российская судебная система пока не в полной мере вовлечена в цифровую модернизацию государственного управления [12]. За период с 2018 по 2023 год наблюдается увеличение количества судебных разбирательств во всех инстанциях: мировых, арбитражных и федеральных судах, на 24%. При этом, наибольшую часть нагрузки (75%) несут мировые суды, которые занимаются разрешением споров, связанных с кредитами, коммунальными платежами и жалобами на действия ФССП. Такая тенденция обусловлена снижением платежеспособности населения и активизацией взыскания задолженностей. Цифровая трансформация судостроения, по мнению СП, пока хромает: закупки оборудования носят хаотичный характер, в эксплуатацию вводится лишь незначительная часть приобретенной техники, а действующие системы функционируют лишь номинально. Отсутствие квалифицированных специалистов для обслуживания оборудования и игнорирование расходов на модернизацию при закупках создают дополнительные препятствия. Несмотря на то, что отдельные цифровые технологии, например, автоматизация внутренних процессов, уже применяются, их широкое внедрение и полное раскрытие потенциала пока не наблюдается. Внедрение системы ГАС «Правосудие» столкнулось с рядом недостатков: ее подсистемы оказались неэффективными, автоматизация процессов не охватила все сферы, а использование устаревшего программного обеспечения влечет за собой значительные финансовые затраты на его поддержку. Инициатива цифровизации Верховного суда, провозглашенная президентскими указами 2015 и 2020 годов, к 2024 году потеряла актуальность, а новые нормативные акты в судебной сфере не были учтены. СП призывает Верховный суд ликвидировать существующие лакуны в нормативно-правовой базе, взять под контроль все ИТ-проекты и создать единые стандарты для оценки уровня цифровизации. Такой подход обеспечит рационализацию бюджетных расходов и интеграцию судов в общенациональную цифровую стратегию.

Действительно, цифровая трансформация сталкивается с рядом препятствий. Физический износ оборудования, моральное устаревание программных продуктов и ограниченность вычислительных мощностей создают серьезные барьеры для развития. Без преодоления этих трудностей полная цифровизация останется лишь утопией.

Отсутствие четкого правового регулирования использования цифровых технологий в судебной системе является актуальной проблемой. Хотя процессуальные кодексы предусматривают возможность дистанционного взаимодействия с судом, вопросы применения, например, искусственного интеллекта,

остаются нерегулируемыми, что порождает опасения у экспертов и правоприменителей.

Заключение. Использование информационно-коммуникационных технологий во всех видах деятельности, в том числе и в юридической, привело к тому, что исследовательский инструментарий, разработанный в качестве методологии в рамках социологии права с момента ее появления, имеет в настоящее время и, как можно предположить, будет иметь и в дальнейшем широкое применение [18. С. 35].

В рамках стратегических планов цифровой трансформации судебной системы, разрабатываемых и утверждаемых судами России совместно с правительством, ключевой задачей является повышение эффективности работы судов. Это стремление к улучшению как качества, так и количества выполняемых судебных функций, а также обеспечение открытости, доступности и прозрачности правосудия для всех. Успешное выполнение поставленных задач в ограниченные сроки достижимо при условии внедрения информационных технологий, отвечающих уровню развития цивилизации. В связи с этим интеграция современных технологических разработок в судебную систему является неотвратимым процессом.

Хотя цифровая трансформация правосудия и новые технологии открывают широкие возможности для защиты прав и участия в судебных процессах, будь то дистанционное обращение в суд или участие в заседаниях, от традиционных способов обращения в судебные органы и участия в судебных разбирательствах пока не стоит отказываться. Введение исключительно электронных и цифровых каналов взаимодействия с судебными органами несовместимо с основополагающими принципами, заложенными в Конституции, и принципами построения и функционирования судебной системы. Успехи цифровой трансформации правосудия тесно связаны с рядом факторов, среди которых стоит отметить «цифровой разрыв», когнитивные возможности и физиологические характеристики граждан, а также технические характеристики предоставления интернет-услуг и других сетей, которые в определенных ситуациях могут ограничивать доступ к правосудию.

Считаем, что в эпоху цифровизации правосудия особую актуальность приобретает задача правового оформления механизмов, которые позволят традиционным правовым нормам и институтам эффективно функционировать в новых реалиях взаимодействия участников правовых отношений. В контексте цифрового правосудия, где информация обрабатывается, хранится и используется в цифровом формате, актуальность вопросов безопасности, прозрачности и юридической ответственности приобретает особую остроту. В эпоху все растущего объема цифровых данных, включая персональные и биометрические данные, необходимо уделять особое внимание защите информационных систем и технологий, а также обеспечить понимание и прозрачность алгоритмов, принимающих решения или предлагающих рекомендации, и четко определить юридическую ответственность за их результаты. Модернизация судебной системы посредством цифровых технологий требует прочного фундамента конституционных норм, обеспечивающих баланс между организационной эффективностью

судопроизводства и соблюдением индивидуальных прав граждан. Процесс технологической трансформации правосудия должен укреплять существующие механизмы судебной защиты населения, а реализация конституционного права граждан на судебную защиту в условиях цифровизации требует разработки дополнительных государственных мер, включающих глубокий анализ специфики работы современных технологических инструментов.

Список литературы

1. Об обеспечении доступа к информации о деятельности судов в Российской Федерации: Федеральный закон от 22.12.2008 № 262-ФЗ (ред. от 14.07.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/ document/cons_doc_LAW_82839/ (дата обращения: 02.09.2025).

2. О федеральной целевой программе "Развитие судебной системы России" на 2007 – 2012 годы: Постановление Правительства РФ от 21.09.2006 № 583 (ред. от 01.11.2012) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_63101/ (дата обращения: 02.09.2025).

3. О федеральной целевой программе "Развитие судебной системы России" на 2002 – 2006 годы: Постановление Правительства РФ от 20.11.2001 № 805 (ред. от 06.02.2004) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34171/ (дата обращения: 02.09.2025).

4. О приостановлении личного приема граждан в судах: Постановление Президиума Верховного Суда РФ, Президиума Совета судей РФ от18.03.2020 № 808 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/ cons_doc_LAW_347974/ (дата обращения: 02.09.2025).

5. О приостановлении личного приема граждан в судах: Постановление Президиума Верховного Суда РФ, Президиума Совета судей РФ от 08.04.2020 № 821 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/ cons_doc_LAW_349751/ (дата обращения: 02.09.2025).

6. В России искусственный интеллект привлекли к вынесению судебных решений // РИА Новости: сайт. URL: https://ria.ru/20210525/intellekt-1733789200.html (дата обращения: 02.09.2025).

7. В Сахалинской области технологии ИИ будут вести протоколы судебных заседаний // Министерство государственного управления Сахалинской области: сайт. URL: https://mingu.sakhalin.gov.ru/press-center/event/v-sahalinskoj-oblasti-tehnologii-ii-budut-vesti-protokoly-sudebnyh-zasedanij (дата обращения: 02.09.2025).

8. Выступление председателя Совета судей Российской Федерации В.В. Момотова на заседании Клуба имени Д.Н. Замятнина по теме: «Электронное правосудие в Российской Федерации: миф или реальность» // Совет Судей Российской Федерации: сайт. URL: https://ssrf.ru/news/vystuplieniia-intierv-iu-publikatsii/42272 (дата обращения: 02.09.2025).

9. Гаджиева Ф.Р., Панкратова Д.А. Перспективы развития электронного правосудия в РФ // Актуальные проблемы современной науки: IV Международная научно-практическая конференция. Ставрополь: Ставропольский университет, 2015. С. 14-19.

10. Жданова Ю.А. Правовая природа электронного правосудия и его место в системе институтов информационного общества // Административное право и процесс. 2015. № 4. С. 80-83.

11. Момотов заявил о переходе к электронному правосудию к 2030 году // РАПСИ: сайт. URL: https://rapsinews.ru/judicial_news/20240402/309776746.html (дата обращения: 02.09.2025).

12. Не в цифре – Счетная палата оценила состояние информатизации судебной системы // Счетная палата Российской Федерации: сайт. URL: https://ach.gov.ru/checks/ne-v-tsifre (дата обращения: 02.09.2025).

13. Работа отечественных судов в условиях пандемии // Верховный Суд Российской Федерации: сайт. URL: https://www.vsrf.ru/press_center/news/28858/ (дата обращения: 02.09.2025).

14. Романенкова С.В. Понятие электронного правосудия, его генезис и внедрение в правоприменительную практику зарубежных стран // Арбитражный и гражданский процесс. 2013. № 4. С 26-31.

15. Российская судебная власть в условиях пандемии // UNODC: сайт. URL: https://www.unodc.org/dohadeclaration/ru/news/2021/06/the-russian-judiciary-in-the-pandemic.html (дата обращения: 02.09.2025).

16. Суддеп: в суды подано 5,5 млн документов в электронном виде // Ассоциация юристов России: сайт. URL: https://alrf.ru/news/suddep-v-sudy-podano-5-5-mln-dokumentov-v-elektronnom-vide/ (дата обращения: 02.09.2025).

17. Цифровизация и электронное дело: новые решения для правосудия будущего // РАПСИ: сайт. URL: https://rapsinews.ru/judicial_news/20250520/310884817.html (дата обращения: 02.09.2025).

18. Галиндо Аюда Ф. Алгоритмы, социология права и правосудие // Journal of Digital Technologies and Law. 2024. Т. 2, № 1. С. 34–45. https://doi.org/10.21202/jdtl.2024.3. EDN: uunzfp.

УДК 347

М. В. Юрченко,
юрист,
ООО «Лидер+»

Развитие цифровых технологий в электронном правосудии в Российской Федерации

Аннотация: В статье рассматриваются вопросы развития цифрового электронного правосудия в Российской Федерации. Автор дает оценку текущему состоянию цифровизации электронного правосудия в Российской федерации, появлению электронного правосудия в Российской Федерации, анализирует существующие системы электронного правосудия «Мой арбитр», ГАС «Правосудие», а также дает рекомендации по дальнейшему развитию электронного правосудия и цифровизации судебной системы и использованию искусственного интеллекта.

Ключевые слова: электронное правосудие, искусственный интеллект, цифровизация, «Legal Tech», «Мой арбитр», ГАС «Правосудие», «Госуслуги»

M.V. Yurchenko,
Lawyer,
LIDER+ LLC

Development of digital technologies in electronic justice in the Russian Federation

Abstract: The article discusses the development of digital e-justice in the Russian Federation. The author assesses the current state of digitalization of e-justice in the Russian Federation, the emergence of e-justice in the Russian Federation, analyzes the existing e-justice systems "My Arbitrator", GAS "Justice", and provides recommendations for the further development of e-justice and the digitalization of the judicial system and the use of artificial intelligence.

Key words: electronic justice, artificial intelligence, digitalization, «Legal Tech», «My Arbitrator», «GAS Pravosudie», «Gosuslugi»

Введение. Актуальность темы статьи обусловлена тем, что в связи с развитием цифровых технологий, развития искусственного интеллекта деятельность юристов становится более автоматизированной. Глобализация и развитие технологий оказали значительное влияние на юридическую практику во всем мире [5. С. 846]. На сегодняшний день «Согласно опросу Legal Insight только 14,5% юристов активно используют инструменты генеративного ИИ, а 33,9% планируют использовать эти инструменты в будущем» [4]. По мнению Колыбиной Е.А. и Воронцова И.В. «В условиях повсеместной цифровизации судеб-

ная система обязана адаптироваться к новым реалиям, чтобы сохранить эффективность и соответствовать потребностям общества» [3 С. 241].

Основная часть. Цифровизация сегодня неотъемлемая, часть юридической деятельности, на сегодняшний день, юристы используют в своей деятельности электронные ресурсы, которые помогают сэкономить время и упростить рутинную работу. Это помогает сосредоточиться на умственной работе, а также экономит время и материальные издержки.

Цель работы: изучить уровень развития цифровизации электронного правосудия в Российской Федерации, а также дальнейшие его развитие.

Задачи:

1. Проанализировать существующие электронные системы правосудия и автоматизированные программы;

2. Предложить рекомендации для дальнейшего развития программ электронного правосудия.

Автоматизация судебной деятельности, в Российской Федерации стала возможной благодаря: техническому оснащению судов компьютерами, развитию электронной почты, появлению сайтов судов, видеосвязи, переходу на электронную систему взаимодействия между судом и участниками процессов. Начало цифровизации дала федеральная целевая программа «Электронная Россия», которая действовала в Российской Федерации в 2002–2010 годах которая была направлена на внедрение технологий «электронного правительства», главная задача переход на предоставление государственных услуг и исполнение государственных функций в электронном виде федеральными органами исполнительной власти [2].

Цифровизация правосудия и развитие электронных систем правосудия способствует быстрому взаимодействию между судами и участниками процессов, а также помогает снизить нагрузки на судебную систему и юристов, также — это помогает снижению потребления бумаги и экономии трудовых ресурсов так как, сотрудникам суда не надо сканировать документы в дело.

Электронное правосудие позволяет сторонам следить за ходом рассмотрения дела онлайн, также оно отражает основы принципы судопроизводства, а именно гласность и равноправие сторон.

Цифровизация правосудия – это современное направление, которое соединяет юридическую деятельность и цифровые технологии и заставляет юристов и сотрудников судов и судьей быть более технологичными в своей деятельности.

В Российской Федерации – существуют системы электронного правосудия: для подачи документов в арбитражные суды «Мой арбитр» которая позволяет полностью взаимодействовать с судами онлайн.

Хронология развития электронных систем правосудия:

1. 2010 год появление портала мировых судей г. Москвы.

2. 2012 год создана система «Мой арбитр».

3. 2016 год появление портала судов общей юрисдикции г. Москвы.

4. В 2017-м появляется электронная система правосудия для судов общей юрисдикции ГАС «Правосудие».

5. 2024 можно подавать документы через «Госуслуги».

Сегодня более развита электронная система правосудия, для арбитражных судов, нежели, для судов общей юрисдикции.

Пандемия 2020 года показала, что в случае необходимости системы модернизуются под условия обстановки в стране, появилась возможность электронного ознакомления и участие в заседаниях электронно.

Также в 2025 году появился диалог с помощью, которого можно задавать 10 бесплатных запросов по делу, а искусственный интеллект даст ответ и краткую инофрмацию по делу.

Согласно национальной стратегии развития искусственного интеллекта на период до 2030 года «искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их» [1].

Нами был проведен опрос посредством Google формы в электронном формате. В опросе приняли участие практикующие юристы, всего опрос прошли 100 человек.

Всего было предложено ответить на семь вопросов:

1. Какими сервисами из перечисленных вы пользуетесь?

– «Госуслуги».
– «Мой арбитр».
– «ГАС Правосудие».
– «Личный кабинет налогоплательщика».
– Другое.

2. Какой сервис для вас самый удобный в использовании?

– «Госуслуги».
– «Мой арбитр».
– «ГАС Правосудие».
– «Личный кабинет налогоплательщика».
– Другое.

3. Укажите кратко достоинства сервиса, который вы выбрали в качестве самого удобного

4. Какой сервис для вас самый НЕ удобный в использовании?

– «Госуслуги».
– «Мой арбитр».
– «ГАС Правосудие».
– «Личный кабинет налогоплательщика»
– Другое.

5. Укажите кратко недостатки сервиса, который вы выбрали в качестве самого НЕ удобного

6. Вы предпочитаете подавать документы и взаимодействовать с государственными органами через личный прием (нарочно) или дистанционно (электронно)?

– личный прием (нарочно).

– дистанционно (электронно).

– Отправляю все по почте.

7. Чтобы вы хотели улучшить в названных сервисах (указать, про какой идет речь) или какой дополнительный сервис вы бы хотели для взаимодействия с государственными органами?

Все респонденты пользуются сервисом «Госуслуги», также большая часть опрошенных пользуется личным кабинетом налогоплательщика, чуть больше половины используют систему «Мой арбитр», и чуть меньше половины пользуются системой «Гас Правосудие», пять указали сервисы, «Casebook», помощник арбитражного управляющего. Надо отметить, что «Госуслуги» – это электронный сервис, которым пользуются все граждане, также через него осуществляется вход в электронные системы правосудия. А электронными сервисами правосудия пользуются участники процессов.

По итогам анкетирования видно, что более многофункциональными в использовании и более технически оснащенными являются портал «Госуслуги» и система «Мой арбитр».

Респонденты отметили такие качества, как удобный интерфейс, письменное уведомление об отправке документов и их регистрации, электронное ознакомление и онлайн заседания, возможность круглосуточной подачи документов, важная информация в одном месте, широкий спектр услуг электронно, хорошо работающий чат-бот, автосохранение черновика и подписка на картотеки с временной отправкой практики на рабочую почту.

Большинство респондентов отметили, что неудобным является сервис «Гас правосудие».

Среди недостатков сложный интерфейс, сложности с ЭЦП, перебои в работе, много информации нужно заполнять, нельзя загрузить все документы, нужно загружать подписывать каждый документ отдельно, «Способ загрузки документов не удобен, суды общей юрисдикции не всегда получают и извлекают из сервиса информацию».

Респонденты взаимодействует с государственными органами и судами, электронно, только 22 % сдают документы нарочно.

На вопрос чтобы вы хотели улучшить в названных сервисах (указать, про какой идет речь) или какой дополнительный сервис вы бы хотели для взаимодействия с государственными органами?

Большинство отметило, уменьшение заполнения карточки, убрать на московском портале судов двойное заполнение (сначала в заявителе, потом в разделе сторон дела, иначе не пропускает система), сделать интерфейс «Гас правосудие» как «Мой арбитр», сделать один портал для подачи документов во все суды.

В качестве дальнейшего развития цифровизации судебной системы видится дальнейшие совершенствование электронных систем правосудия, например в системе «Мой арбитр»:

1) сделать маркировки в карточке дела о подаче документов в электронном виде или бумажном, чтобы было ясно, как поданы документы и отпала необходимость звонить в суд и спрашивать;

2) сделать возможность оплаты госпошлины при подаче иска в суд сразу;

3) ознакомление с обособленными спорами в банкротстве сделать маркировку по спорам сейчас непонятно, какой документ поступил в какой спор и нужен ли он, участнику конкретного спора;

4) необходимость подавать ходатайство об ознакомлении на электронное ознакомление, можно сделать что участники по делам имели доступ до его рассмотрения в гражданских спорах и административных, а в банкротных по сделкам, если лицо, например, участвует в конкретной сделке, а не кредитор или не должник;

5) упростить подачу заявления на онлайн заседание, если лицо участвует одно и то же, то можно просто повторить заявление, а не прикреплять все документы по новой или сделать вкладку, что при отложении, если это же лицо потом участвует, то ставит галочку;

6) возможность скачать документы в рамках гражданских дел и административных одним архивом;

7) автоматически предлагать выдачу исполнительного листа по гражданским делам без надобности подавать заявление по окончанию рассмотрения иска;

8) возможность электронной записи на нарочное ознакомление можно выбрать при подаче заявке как сейчас ставим галочки электронное нарочное, так и тут можно выбрать нарочно и конкретный день и время.

В рамках системы «Гас правосудие» — это развитие электронного ознакомления с материалами дела и появление электронных заседаний.

Заключение. В будущем видится возможным внедрение искусственного интеллекта в приказном производстве, для снижения нагрузки на судей, сегодня большая часть нагрузки на судей – это приказное производство, поэтому снижение доли рассмотрения приказов судьями и передача их на рассмотрение искусственному интеллекту поможет снизить нагрузку на судей, а также начать применять искусственный интеллект, для регистрации документов поступающих в суд электронно через системы электронного правосудия по заданному алгоритму и шаблону, ввиду высокой нагрузки на сотрудников судов, данные действия помогут снизить нагрузку у судей и сотрудников суда.

Список литературы

1. Указ Президента РФ от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

2. Постановление Правительства Российской Федерации от 28.01.2002 № 65 «О федеральной целевой программе «Электронная Россия» (2002-2010 годы) // Собрание законодательства РФ.2002. № 5. Ст. 531.

3. Колобынина Е.А., Воронцова И.В. Влияние цифровизации на гласность правосудия//Международный журнал гуманитарных и естественных наук. 2025. №1-1 (100). С. 241-244.

4. РБК Искусственный интеллект для юристов: как развивается сфера Legal AI новость от 15.07.2025. URL: https://trends.rbc.ru/trends/innovation/687110ec9a79478fa6d8db5a (дата обращения 07.09.2025).

5. Икубанни О.О., Ойебанджи А.О., Ойебаде А.А. Юридические аспекты наделения искусственного интеллекта субъектностью: перспективы использования роботов в юридической практике в Нигерии // Journal of Digital Technologies and Law. 2024. Т. 2, № 4. С. 835-856. URL: https://doi.org/10.21202/jdtl.2024.41. EDN: FHNKJQ.

УДК 34

В. А. Якимчук,
аспирант,
Российский государственный педагогический университет
имени А.И. Герцена

Правосудие в эпоху цифровизации: проблемы и решения для внедрения международных норм борьбы с коррупцией

Аннотация. В статье рассматриваются текущие вопросы правосудия в контексте цифровизации, а также проблемы, связанные с реализацией международных антикоррупционных стандартов. В эпоху быстрого развития информационных технологий и цифровых платформ правовые системы сталкиваются с новыми угрозами, которые требуют адаптации существующих правоохранительных механизмов. Основное внимание уделяется анализу влияния цифровизации на коррупционные практики, а также на изучение существующих международных стандартов и инициатив, направленных на их профилактику. В статье предлагается комплексный подход к решению выявленных проблем, включая рекомендации по повышению прозрачности судебных разбирательств, внедрению систем электронного мониторинга и укреплении сотрудничества между государственными учреждениями и гражданским обществом. Особое внимание уделяется роли технологий в повышении эффективности исследований и испытаний. В статье подчеркивается необходимость интеграции международных норм в национальные правовые системы, что создаст более устойчивую и справедливую судебную практику в контексте цифровой трансформации.

Ключевые слова: право, цифровые технологии, коррупция, правосудие, международные стандарты, закон, международные нормы, борьба с коррупцией

V. A. Iakimchuk,
3rd year postgraduate student, Department of International Law,
Faculty of Law, A.I. Herzen Russian State Pedagogical University

Justice in the age of digitalization: Problems and solutions for the implementation of international anti-corruption standards

Abstract. The article examines the current issues of justice in the context of digitalization, as well as the challenges associated with the implementation of international anti-corruption standards. In the era of rapid development of information technologies and digital platforms, legal systems are faced with new threats that require the adaptation of existing law enforcement mechanisms. The main focus is on the analysis of the impact of digitalization on corrupt practices, as well as the study of existing international standards and initiatives aimed at their prevention. The article offers a comprehensive approach to solving the identified problems, including rec-

ommendations for improving the transparency of judicial proceedings, introducing electronic monitoring systems and strengthening cooperation between government institutions and civil society. Particular attention is paid to the role of technology in increasing the effectiveness of investigations and trials. The article emphasizes the need to integrate international norms into national legal systems, which will create a more sustainable and fair judicial practice in the context of digital transformation.

Keywords: law, digital technologies, corruption, justice, international standards, law, international norms, fight against corruption

Введение. Цифровизация правосудия представляет собой один из наиболее значимых веяний современности, которое оказывает глубокое влияние на деятельность судебных систем во всем мире. В условиях глобализации и стремительного развития технологий, внедрение международных норм борьбы с коррупцией становится неотъемлемой частью для обеспечения справедливости и правопорядка повсеместно. Коррупция, являясь одной из основных угроз стабильности и развития государств, нуждается в комплексном подходе, включающим в себя адаптацию международных стандартов к новым цифровым реалиям. Но тем не менее процесс цифровизации правосудия сталкивается с серьезными проблемами, такими как недостаточная инфраструктура, правовые барьеры, вопросы безопасности данных и защиты прав граждан.

Основная часть. Несмотря на то, что цифровизация правосудия открывает перспективы для борьбы с коррупцией, она также ставит перед нами ряд серьезных вызовов. Имплементация международных норм, помимо технических решений, также требует комплексного подхода к правовым, этическим и социальным направлениям. Необходимость создания устойчивой инфраструктуры, безопасности данных и защита прав граждан становится весьма актуальной в условиях стремительного изменения технологий. Значимым этапом к успешной интеграции международных стандартов является развитие сотрудничества между странами, а также обмен опыта лучших практик. Государствам следует адаптировать свои законодательные системы к современным реалиям, обеспечивая прозрачность и подотчетность органов правосудия.

Таким образом, цифровизация может стать внушительным инструментом в борьбе с коррупцией, если будет сочетаться с конкретными стратегиями и политической волей. Применение современных технологий должно идти бок о бок с укреплением правовых основ, что, в свою очередь, позволит создать справедливую и эффективную судебную систему в век цифровых технологий.

Цифровизация в правосудии охватывает широкий спектр инициатив и инструментов, включая электронные судебные дела, онлайн-услуги для подачи исков, видеоконференции для судебных слушаний, а также внедрение искусственного интеллекта для анализа судебной практики [2]. Этот процесс не только трансформирует методы взаимодействия между судами и гражданами, но и меняет суть работы правоохранительных органов, позволяя создавать более динамичные и адаптивные системы.

Важным аспектом цифровизации является необходимость соблюдения принципов верховенства закона и защиты прав человека. Это означает, что лю-

бые технологии, введенные в судебную систему, должны соответствовать международным стандартам прав человека и защищать данные граждан. Основываясь на этом, цифровизация правосудия не только упрощает доступ к юридическим услугам, но и требует внимательного отношения к этическим и правовым вопросам. Цифровизация правосудия включает несколько ключевых областей [6. С. 4-6], каждая из которых играет немаловажную роль в создании более эффективной и прозрачной судебной системы:

1. Электронное судопроизводство. Одно из важных достижений цифровизации является переход к электронному судопроизводству. Это включает в себя возможность подачи исков, документов и других материалов в электронном виде, что значительно сокращает время для обработки дел и сводит к минимуму бумажный документооборот. Электронные базы данных позволяют быстро найти необходимую информацию и отслеживать статус дел.

2. Использование технологий для повышения доступа к правосудию. Цифровизация также предоставляет современные средства для доступа к правосудию, особенно для уязвимых групп населения. Онлайн-платформы могут предлагать юридические консультации, помощь в подготовке документов и доступ к информации о правах граждан. Это особенно важно в условиях ограниченного доступа к юридическим услугам в отдаленных или неблагоприятных областях.

3. Видеоконференции и дистанционные участие. Внедрение технологий видео коммуникаций позволяет участникам судебного разбирательства (судьям, адвокатам, свидетелям и пр.) принимать участие в заседаниях без необходимости физического присутствия в зале суда. Это не только снижает транспортные расходы, но и делает судебные процессы более гибкими и доступными.

4. Искусственный интеллект и аналитика данных. Искусственный интеллект (далее – ИИ) начинает играть все более важную роль в анализе судебной практики и предсказании исходов дел. Алгоритмы могут обрабатывать большие объемы данных, идентифицируя закономерности и направления, что помогает судьям принимать более рациональные решения. Однако, в связи с тем, что ИИ не полностью изучено, его использование также поднимает вопросы о прозрачности методов и возможности предвзятости.

5. Кибербезопасность и защита данных. При увеличении объема обрабатываемой информации растет необходимость улучшения обеспечения безопасности данных. Судебные системы обязаны быть защищены от кибератак, а также гарантировать конфиденциальность личных данных граждан. Это требует введения современных технологий защиты данных и постоянного мониторинга угроз.

6. Обучение и повышение квалификации кадров. Для успешной реализации цифровизации необходимость обучения судебных сотрудников новым технологиям и методам работы стремительно растет. Это включает в себя как технические навыки, так и понимание юридических аспектов использования цифровых инструментов.

Цифровизация правосудия и практики правоохранительных органов открывает новые горизонты для борьбы с коррупцией, но она также ставит ряд

серьезных проблем перед обществом и государственными институтами [1. С. 51]. Внедрение международных норм и стандартов в условиях быстрой цифровизации требует интегрированного подхода, который учитывает как технические, так и юридические, социальные, а также культурные аспекты. Одной из основных сложностей внедрения международных норм в условиях цифровизации является наличие технических проблем, и недостатков инфраструктуры. Это относится как к физическим, так и к программным компонентам цифровых систем.

Во многих развивающихся странах существуют существенные расхождения в доступе к современным технологиям [7]. Это может быть связано с недостаточным финансированием, отсутствием необходимых технических знаний у персонала или несовременной инфраструктурой. следствие, судебные и правоохранительные органы могут просто не иметь возможности эффективного использования цифровых инструментов для борьбы с коррупцией. Различные страны могут использовать отличные системы и системы для управления судебными процессами и правоприменением. Это создает проблемы совместимости, что усложняет обмен информацией между государствами и внедрением международных стандартов. Без единых решений трудно обеспечить эффективное взаимодействие между различными юрисдикциями в борьбе с транснациональной коррупцией. Цифровизация также открывает «беспомощность» в системе правосудия. Кибератаки могут быть серьезной опасностью для целостности данных, а также для работы судебных систем. Если система не может быть должным образом защищена, это может привести к утечке конфиденциальной информации, махинациям с данными или даже фальсификации доказательств.

Во многих странах законодательства не успевают за интенсивным ростом цифровизации. Устаревшие законы могут не учитывать технологии и методы работы, что усложняет их применение в современных условиях. Это создает юридические пробелы, которые можно использовать в коррупционных системах. Имплементация международных норм требует гармонизации национального законодательства с международными стандартами. Это трудный процесс, особенно если дело касается стран с устоявшимися правовыми традициями. Необходимость внести изменения в законодательство может вызвать противоречия со стороны заинтересованных лиц.

Таким образом, внедрение международных норм в контексте цифровизации является сложным процессом, который требует интегрированного подхода к решению возникающих проблем. Технические проблемы, правовые и институциональные барьеры, социальные и культурные аспекты, а также проблемы безопасности данных требуют тщательного анализа и разработки эффективных стратегий для их преодоления.

Коррупция остается одной из основных проблем, с которыми сталкиваются страны мира. Основным шагом к эффективной борьбе с коррупцией является адаптация законодательства. Устаревшие законы, не учитывающие современные реалии, могут создавать правовые пробелы, которыми злоумышленники используют в своих интересах вопреки интересам общества. Необходимо проанализировать существующие нормы и определить их недостатки, а затем разрабо-

тать новые и обновлять существующие законы, чтобы они могли полностью или частично соответствовать международным стандартам.

Должны быть имплементированы международное антикоррупционные стандарты и рекомендации, содержащиеся в Конвенции Организации Объединенных Наций против коррупции и других региональных соглашениях. Необходимо разработать структуру специализированных органов для борьбы с коррупционными преступлениями, которые будут расследовать и преследовать коррупционные преступления. Эти органы должны быть независимыми и иметь все необходимые полномочия для выполнения своих основных обязанностей, а также иметь финансовую и кадровую поддержку.

За последнее десятилетие цифровизация стала существенным инструментом в борьбе с коррупцией, предоставляя новые возможности для повышения прозрачности, ответственности и эффективности государственных процессов. Ни одна страна, ведущая борьбу с коррупцией смогла достичь значительных успехов в устранении проблемы. Так, например, Сингапур, известный своей строгой антикоррупционной политикой и эффективными механизмами контроля, использует технологии для мониторинга и анализа данных, что позволяет выявлять подозрительные финансовые операции и коррупционные схемы. Власти Сингапура используют алгоритмы для анализа финансовых потоков и выявления аномалий, указывающих на коррупционные правонарушения. Кроме того, граждане могут сообщать о коррупционных действиях через мобильное приложение, которое помогает повысить уровень участия населения в борьбе с коррупцией, а также регулярные тренинги для сотрудников государственных органов по использованию технологий в борьбе с коррупцией помогают повысить их квалификацию и эффективность работы [9].

Также как и Сингапур, большие успехи в использовании цифровизации в борьбе с коррупцией имеют такие страны, как Индия, Кения, Грузия и пр. Из примера этих стран можно сделать вывод, что ключевым фактором в борьбе является прозрачность. Цифровые технологии позволяют сделать процессы более открытыми и доступными для граждан. Это не только снижает вероятность коррупционных действий, но и повышает доверие населения к государственным институтам.

Введение цифровых технологий в борьбу с коррупцией является мощным инструментом повышения прозрачности, ответственности и эффективности государственных процессов. Примеры успешной практики из разных стран говорят нам о том, что такие меры могут сократить коррупцию и повысить доверие граждан к государственным учреждениям [4. С. 23-24].

В заключение следует отметить, что эра цифровизации является не только вызовом, но и возможностью для системы правосудия и борьбы с коррупцией. С одной стороны, быстрое развитие технологий, таких как блокчейн и искусственный интеллект, например, открывает новые горизонты для увеличения потоков, автоматизации процессов и обеспечения более высокого уровня доступа к информации, что является ключевым аспектом в борьбе с коррупцией. С другой стороны, цифровизация также привносит новые проблемы, связанные с безопасностью данных, защитой конфиденциальной информации и возможностью

манипуляций с цифровыми системами. Увеличение объема информации и сложность ее обработки требуют, чтобы правовые системы адаптировались к новым реалиям, что может послужить серьезным препятствием для эффективного применения международных стандартов борьбы с коррупцией. Важно отметить, что стандартные подходы к правосудию могут быть неэффективными в контексте быстрого изменения технологической среды.

Для успешной имплементации международных норм в борьбе с коррупцией в эпоху цифровизации необходимо разработать интегрированный подход, который будет объединять законодательные инициативы, технические решения и образовательные программы. Важно создать правовую основу, которая будет учитывать особенности цифровой экономики и обеспечивать защиту прав граждан. Это может включать в себя разработку новых законов о кибербезопасности, защите конфиденциальных данных, прозрачности государственных закупок и пр. Более того, необходимо активное сотрудничество между государственными органами, частным сектором и гражданским обществом. Обмен опытом и лучшими практиками на международном уровне существенно улучшит и выработает эффективные стратегии борьбы с коррупцией в контексте цифровизации. Одним из важных моментов этого процесса является повышение уровня осведомленности граждан о проблемах коррупции и важности соблюдения норм правосудия.

Внедрение новых технологий должно сопровождаться строгим контролем и оценкой их эффективности. Необходимо разработать механизмы мониторинга и оценки реализованных решений для обеспечения соотношения их международным стандартам. Также важно учитывать необходимость защиты прав человека во время цифровизации во избежании потенциальных нарушений и злоупотреблений [3. С. 164].

Заключение. Таким образом, успешная интеграция международных норм борьбы с коррупцией в эпоху цифровизации требует интегрированного подхода, включая законодательные изменения, применение современных технологий, а также активное взаимодействие всех заинтересованных сторон. Только в этом случае можно создать эффективную систему правосудия, которая может противостоять проблемам современности и обеспечить справедливость в обществе. В конечном счете введение инновационных решений в борьбе с коррупцией не только повысит доверие граждан к государственным органам, но также станет значимым шагом на пути к стабильному развитию и процветанию общества в целом.

Список литературы

1. Бурдина Е. В. Цифровой доступ к суду в Российской Федерации: концепция, цели, содержание // Российский судья. 2022. № 10. С. 49–53.

2. Корякин В. М. «Цифровизация» общественных отношений и ее влияние на состояние коррупции в военной организации государства // Военное право. 2019. № 1 (53).

3. Овсянников А. И. Противодействие коррупции в условиях цифровизации: возможности, перспективы, риски // Журнал Российского права. 2019. № 11. С. 158–170.

4. Романовская О. В. Романовская Е. А. Правовой режим цифровой юстиции: проблемы и перспективы // Электронный научный журнал «Наука. Общество. Государство». 2024. Т. 12. № 1. URL: https://esj.pnzgu.ru (дата обращения: 01.09.2025).

5. Солохин А.Е. Электронное правосудие: особенности, проблемы и перспективы // Закон. 2019. № 6. С. 193-208.

6. Velibor Božić The Role of Artificial Intelligence in Reducing Corruption in Smart Cities, 1-15. 2025.

7. European Commission. AI for Smart Cities: Ethical Guidelines and Best Practices. Brussels: EU Publications Office. 2022.

8. World Bank. Leveraging Technology for Transparency and Anti-Corruption in Urban Governance. Washington, DC: World Bank Group. 2023.

9. Transparency International. Global Corruption Report: Smart Cities and AI. Berlin: Transparency International.2024.

УДК 343.97

М. Р. Нигматуллин,
преподаватель,
Тюменский институт повышения квалификации
сотрудников МВД России

Цифровое насилие в отношении женщин: уголовно-правовые и виктимологические аспекты

Аннотация. Эпоха цифровизации, наряду с неоспоримыми преимуществами, создала новые формы социально опасного поведения. В данной статье рассматривается проблема цифрового насилия в отношении женщин, как социальная и правовая проблема современного информационного общества. Проводится анализ ключевых форм цифрового насилия, в частности, совершаемых исключительно в отношении женщин, таких как апскертинг (upskirting), крипшот (creepshot), порноместь (revengeporn) и сексторшен (sextortion). Цифровое насилие может иметь долгосрочные негативные последствия для социальных отношений, карьеры и общего благополучия жертвы. В статье также затрагиваются вопросы правового регулирования: автором предлагается внести изменение в статью 137 Уголовного кодекса Российской Федерации.

Ключевые слова: цифровое насилие, дипфейк, апскертинг, крипшот, порноместь, сексторшен

M. R. Nigmatullin,
lecturer,
Tyumen Institute for Advanced Training of Employees
of the Ministry of Internal Affairs of Russia

Digital violence against women: criminal and victimologicak aspects

Abstract. The digital era, along with its undeniable advantages, has given rise to new forms of socially dangerous behavior. This article examines the problem of digital violence against women as a social and legal problem of the modern information society. An analysis of key forms of digital violence is provided, in particular thosecommitted exclusively against women, such as upskirting, creepshot, revenge porn, and sextortion. Digital violence can have long-term negative consequences for social relationships, career, and overall well-being of the victim. The article also addresses issues of legal regulation; the author proposes to amend Article 137 of the Criminal Code of the Russian Federation.

Keywords: digital violence, deepfake, upskirting, creepshot, revenge porn, sextortion

Введение. Цифровое насилие в Российской Федерации долгое время игнорировалось и не воспринималось всерьез. Это объяснялось недостаточным пониманием специфики данного социально опасного явления, сложностью квалификации и привлечения виновных лиц к юридической ответственности [3]. Однако в последние годы, благодаря усилиям правозащитных организаций и ряда исследователей, удалось сформировать общественное мнение о цифровом насилии как о серьезной угрозе для безопасности и благополучия граждан, особенно женщин и детей. Публичные дискуссии, научные публикации и исследования способствовали повышению осведомленности о различных формах цифрового насилия, таких как кибербуллинг, сталкеринг, распространение интимных материалов без согласия и др. [7].

Основная тема. Тема цифрового насилия постепенно становится частью публичного дискурса и повестки дня. Сегодня активно продвигаются идеи о необходимости криминализации новых форм насилия, совершаемых с использованием цифровых технологий. Сейчас происходит переосмысление понятия цифрового насилия, расширение его границ и адаптация правовой системы к реалиям цифровой эпохи. Различные формы цифрового насилия, будь то кибербуллинг, сексторшен, распространение интимных материалов без согласия или онлайн-харассмент, подрывает чувство безопасности и доверия к окружающему миру. Жертвы цифрового насилия часто ощущают себя беспомощными, уязвимыми и неспособными контролировать ситуацию, что может привести к серьезным эмоциональным и психологическим травмам.

Согласно информации, опубликованной американским аналитическим центром Pew Research Center, «40 % интернет-пользователей хотя бы раз сталкивались с проявлениями агрессии в цифровой среде, а 73 % были сторонними наблюдателями подобных ситуаций. В подавляющем большинстве случаев (66 %) платформой для таких инцидентов становятся социальные сети. Наиболее часто жертвами цифрового насилия становится молодые люди в возрастной категории от 18 до 29 лет, с этим явлением сталкиваются около 70 % интернет-пользователей. Особенно подвержены риску стать жертвой цифрового насилия девушки в возрасте от 18 до 24 лет. Согласно статистике, 26 % сталкивались с онлайн-преследованиями, а каждая четвертая (25 %) подвергалась сексуальным домогательствам в интернете» [7].

Исходя из публикации Forbes Woman, следует, что значительная часть (60 %) интернет-пользователей, ставших жертвами цифрового насилия, предпочитают не реагировать на нее. Однако оставшиеся 40 % активно сопротивляются, чаще всего отвечая агрессорам или блокируя их аккаунты. При этом лишь четверть женщин, столкнувшихся с неправомерными действиями в сети Интернет, обращаются с жалобой к администраторам онлайн-платформ. Большинство пострадавших предпочитают искать поддержку среди своих близких, так как привлечь лицо к ответственности не всегда возможно. Примечательно, что в 54 % случаев женщины, подвергшиеся цифровому насилию, знакомы со

своим обидчиком. Важно отметить, что цифровое насилие нередко сопутствует романтическим отношениям и часто сочетается с другими формами насилия [10].

В зарубежной англоязычной юридической и психологической литературе употребляется несколько терминов, относящихся к цифровому насилию. Помимо цифрового насилия, подразумевающего насилие в онлайн среде, употребляются также специальные термины, относящиеся только к женщине: апскертинг (upskirting) и крипшот (creepshot) – фотографирование интимных частей тела незнакомой женщины или партнерши без согласия; порноместь (revengeporn) – распространение интимных изображений или видеозаписей человека без его согласия с целью унижения, шантажа или причинения морального вреда, как правило совершенных по мотиву мести или личных неприязненных отношений; сексторшен (sextortion) – это форма шантажа или вымогательства, при которой злоумышленник угрожает распространить интимные фотографии или видео потерпевшей, если последняя не выполнит их требования [10].

Эти формы цифрового насилия, нацеленные именно на женщин, подчеркивают гендерность указанной проблемы. Важно отметить, что цифровое насилие не ограничивается этими конкретными примерами. Оно может принимать различные формы, включая кибersталкинг, доксинг (публикация личной информации), онлайн-харассмент и другие действия, направленные на причинение вреда, унижение или запугивание жертвы. В юридическом контексте важно обеспечить адекватную защиту жертв цифрового насилия и привлечение виновных к ответственности. Законодательство должно быть адаптировано к новым формам насилия, возникающим в цифровой среде, и предусматривать эффективные меры для предотвращения и противодействия этим явлениям.

К тому же с развитием искусственного интеллекта возрастает опасения относительно личной безопасности и сохранности персональной информации. В частности, такие цифровые технологии как deepfake использует сложные алгоритмы машинного обучения, которые обучаются на огромных массивах данных, состоящих из изображений и звуков реальных людей, чтобы затем имитировать их внешность и голос с поразительной точностью. Кроме того, нейронные сети способны генерировать абсолютно новый контент, в котором люди предстают в различных ситуациях или произносят фразы, которые никогда не имели места в действительности [1. С. 452].

Первые проявления deepfake привлекли внимание общественности в 2017 году, когда в интернете начали появляться видеоролики, в которых лица знаменитостей были наложены на тела порноактрис. Это вызвало волну возмущения и опасений относительно возможности использования технологии для распространения дезинформации и клеветы. Однако с тех пор deepfake вышел далеко за рамки порнографии и стал применяться в самых разных сферах. Deepfake несет в себе огромный потенциал для образовательных, художественных и иных целей [2. С. 30].

К сожалению, вместе с возможностями технология deepfake приносит и серьезные риски. Самая очевидная опасность – это распространение дезинфор-

мации и фейковых новостей. Другой риск связан с подменой личности. Deepfake может быть использован для обмана систем распознавания лиц, получения доступа к личной информации или совершения мошеннических действий. Нередко мошенники используют голос человека, скопированный с помощью deepfake, для обмана его родственников или друзей, выманивая у них денежные средства под предлогом необходимости оказания срочной материальной помощи.

Сама разработанность категориального аппарата, связанного с цифровым насилием, указывает на значительный интерес к данной проблеме. Самый распространенный термин в российской специальной литературе – цифровое насилие. Э.Л. Сидоренко определяет цифровое насилие как онлайн-воздействие на лицо либо группу лиц против либо вопреки их воли, которое совершается при помощи информационно-коммуникационных технологий с целью причинения вреда или угрозы его причинения физическим лицам, что в последствии приводит или может привести к причинению психологического, физического и экономического ущерба [8. С. 72].

Определение цифрового насилия, предложенное Э.Л. Сидоренко, акцентирует внимание на использовании информационно-коммуникационных технологий как инструмента для причинения вреда, подчеркивая при этом элемент недобровольного воздействия на жертву. Это определение охватывает широкий спектр действий, от психологического давления до экономического ущерба, что отражает многогранность онлайн-среды и потенциальные последствия таких действий.

Например, С.А. Стяжкина считает, что под информационным насилием следует понимать воздействие на личность, подавляющее его волю и принуждающее к определенному, противоправному или аморальному поведению, причиняющее вред его психическому и физическому здоровью, а также нравственному развитию [9. С. 724]. Подход данного автора, рассматривающего информационное насилие как форму воздействия, подавляющую волю и принуждающую к нежелательному поведению, делает акцент на моральном и этическом аспектах. В данном контексте насилие рассматривается не только как причинение вреда здоровью, но и как нарушение нравственных принципов.

Несмотря на многообразие формулировок, ключевым элементом определения цифрового насилия является использование информационно-коммуникационных технологий как инструмента для причинения вреда. По нашему мнению, под цифровым насилием следует понимать виновное противоправное деяние, причиняющие неимущественный и/или имущественный вред личности или создающее угрозу причинения такого вреда, совершенное с помощью информационно-коммуникационных технологий.

Осознание многообразия цифрового насилия и его проявлений является ключевым моментом для создания эффективных мер профилактики и защиты от цифрового насилия. Важно расширять знания о потенциальных угрозах, сопряженных с применением современных информационных технологий. Особенностью цифрового насилия является его потенциально неограниченная аудитория и скорость распространения информации. Сообщения и материалы,

содержащие оскорбления, угрозы или клевету, могут мгновенно распространиться среди множества пользователей, нанося значительный вред деловой репутации, чести, достоинству и психическому здоровью жертвы. Важно осознавать, что цифровое насилие является серьезной проблемой, требующей комплексного подхода к ее предотвращению и пресечению.

В уголовном кодексе Российской Федерации (далее также – УК РФ) предусмотрен ряд норм, в которых закреплена ответственность, подпадающая под определение цифрового насилия. В первую очередь это ч. 2 ст. 128.1 УК РФ – клевета, совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет». При рассмотрении уголовных дел о клевете, совершенной в сети Интернет, суды учитывают такие факторы, как контекст высказывания, его форму, степень публичности и возможные последствия для потерпевшего. Важно отличать клевету от оценочных суждений, которые не могут быть предметом судебного разбирательства, если они не содержат заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию. Дела о клевете, совершенной в сети Интернет, часто сопряжены с трудностями в установлении личности распространителя информации, особенно если используются анонимные аккаунты или поддельные профили.

Нередко в судебной практике встречаются случаи, когда один из бывших супругов (сожителей) или сексуальных партнеров, движимый местью за разрыв отношений, выкладывает в открытый доступ – в социальные сети или на другие интернет-платформы – интимные фото- или видеоматериалы, на публикацию которых согласия не давалось. Такие факты в настоящее время квалифицируются по ст. 137 УК РФ (нарушение неприкосновенности частной жизни). Н.А. Конорезов справедливо отметил, что распространение соответствующих сведений о частной жизни лица «в информационно-телекоммуникационных сетях, включая сеть Интернет» не является конструктивным признаком состава преступления, предусмотренного ст. 137 УК РФ. Законодатель ограничился указанием лишь на совершение названного деяния в средствах массовой информации [5. С. 143].

Кроме того, сегодня сеть Интернет играет важную роль и является незаменимым инструментом для получения информации, глобального общения, образования, бизнеса, развлечений и его отсутствие в тексте диспозиции ст. 137 УК РФ может рассматриваться как несоответствие современным реалиям. Учитывая развитие информационных технологий и широкое распространение цифрового контента, необходимо рассмотреть возможность введения в УК РФ о квалифицирующего признака указанной статьи, предусматривающей ответственность за распространение интимных изображений и видео без согласия лица, изображенного на них (так называемый «revengeporn»). Такая норма позволила бы учесть специфику данного вида преступлений, а также предусмотреть более строгие санкции, соразмерные причиненному вреду.

Нередко для получения доступа к конфиденциальным данным преступники используют различные тактики: от взлома личных устройств и аккаунтов до эксплуатации доверительных отношений [11. С. 134]. Анонимность в интер-

нете способствует распространению таких действий, усложняя идентификацию и привлечение виновных к ответственности. Частным примером подобного вымогательства является сексторция (сексторшн), когда злоумышленники угрожают распространить интимный контент в информационно-телекоммуникационной сети Интернет, если жертва не выполнит определенные требования. В ряде случаев под сексторцией понимают «мошенническую схему, когда пользователю рассылают спам-сообщения, убеждающей пользователя, что у недоброжелателей есть компрометирующие его съемки во время посещения порносайтов». Согласно отчету компании ESET, 11 % пользователей сети были объектами таких «сексуальных вымогательств» [4. С. 91].

В случае если лица используют шантаж с целью получения от потерпевшего сексуальных услуг, данное деяние квалифицируется по ст. 133 «Понуждение к действиям сексуального характера», если требуют имущество либо денежные средства – по ст. 163 УК РФ «Вымогательство». Важно отметить, что в п. 12 Пленума Верховного Суда Российской Федерации постановления от 17 декабря 2015 г. № 56 «О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации) обращает внимание судов на то, что по смыслу части 1 статьи 163 УК РФ под сведениями, позорящими потерпевшего или его близких, следует понимать сведения, порочащие их честь, достоинство или подрывающие репутацию (например, данные о совершении правонарушения, аморального поступка). При этом не имеет значения, соответствуют ли действительности сведения, под угрозой распространения которых совершается вымогательство [6].

Важно разграничивать вымогательство от других преступлений, таких как клевета или оскорбление. Вымогательство характеризуется, прежде всего, намерением получения имущества, как правило денежных средств или совершения других действий имущественного характера под угрозой распространения позорящих потерпевшего или его близких сведений. В то время как клевета и оскорбление преследуют цель унизить или опорочить честь и достоинство личности. Таким образом, при квалификации вымогательства необходимо установить намерение виновного получить имущественную выгоду или совершить действия имущественного характера под угрозой распространения сведений, порочащих потерпевшего или его близких.

Обобщая результаты проведенного анализа цифрового насилия, можем сделать следующие выводы:

1. Трактовка понятий цифрового насилия подразумевает собой совершение преступлений с использованием информационно-коммуникационных технологий. Таким образом, основным объектом указанных преступлений могут быть различные общественные отношения, где информационно-коммуникационные технология выступают способом совершения преступления.

2. В правоприменительной и судебной практике имеется отражение следующих видов (типов) цифрового насилия:

– склонение к совершению самоубийства или содействие совершению самоубийства в информационно-телекоммуникационных сетях (включая сеть «Интернет» (ч. 3 ст. 110 УК РФ);

– клевета, совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» (ч. 2 ст. 128.1 УК РФ);

–понуждение к действиям сексуального характера с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет» (ч. 3 ст. 133 УК РФ);

– нарушение неприкосновенности частной жизни (ст. 137 УК РФ);

– нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ);

– вымогательство под угрозой распространения позорящих потерпевшего или его близких сведений (ст. 163 УК РФ) и др.

3. Предлагаем внести изменения в часть 1 статьи 137 УК РФ и дополнить ее следующим текстом «либо в информационно-телекоммуникационных сетях, в том числе сети «Интернет»:

УК РФ Статья 137. Нарушение неприкосновенности частной жизни

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, средствах массовой информации **либо информационно-телекоммуникационных сетях, в том числе сети «Интернет»**, за исключением случаев, предусмотренных статьей 272.1 настоящего Кодекса.

4. Правовой анализ показывает, что существующее уголовное законодательство в недостаточной мере охватывает все формы цифрового насилия, что в ряде случаев приводит к безнаказанности виновных и отсутствию эффективной защиты прав интернет-пользователей. Правоприменительная и судебная практика, как в случае Валерии Володиной, сталкивается с отказами в возбуждении дел или их прекращением. Недостаточно четкое определение границ дозволенного поведения в цифровой среде создает трудности в квалификации преступлений и доказывании вины.

В связи с этим возникает необходимость разработки комплексных мер по противодействию цифровому насилию, включающих в себя совершенствование законодательства, повышение правовой грамотности населения и создание эффективных механизмов защиты прав потерпевших. Особое внимание следует уделять профилактике цифрового насилия в отношении уязвимых групп населения, таких как женщины и дети.

Список литературы

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

2. Воронин В.И., Гавра Д.П. Дипфейки: Современное понимание, подходы к определению, характеристики, проблемы и перспективы // Российская школа связей с общественностью. 2024. № 33. С. 28-47.

3. ЕСПЧ защитил россиянку от кибербуллинга // Правовые новости. URL:https://pravo.ru/news/234762/ (дата обращения: 28.08.2025).

4. Жмуров Д.В. Кибервиктимология вымогательств в цифровом пространстве // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. № 2. С. 85-98.

5. Конорезов Н.А. Уголовно-правовая характеристика нарушения неприкосновенности частной жизни в сети Интернет // Гуманитарные, социально-экономические и общественные науки. 2023. № 3. С. 142–145.

6. О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации): Постановление Пленума Верховного Суда Рос. Федерации от 17 дек. 2015 г. № 56 // СПС КонсультантПлюс[Электронный ресурс] (дата обращения: 28.08.2025).

7. Онлайн преследование // Исследовательский центр Пью (PewResearchCenter). URL: https://www.pewresearch.org/ internet/2014/10/22/part-2-the-online-environment/ (датаобращения: 28.08.2025); HenryN, PowellA. Technology-FacilitatedSexualViolence: ALiteratureReviewofEmpiricalResearch. Trauma Violence Abuse. 2018 Apr;19(2):195-208. doi: 10.1177/1524838016650189. Epub 2016 Jun 16. PMID: 27311818 др.

8. Сидоренко Э.Л. Цифровое насилие в отношении детей: понятие, виды и особенности квалификации // Lex russica. 2024. № 12. С. 68-83.

9. Стяжкина С.А. Уголовная ответственность за информационное насилие: проблемы криминализации и систематизации // Вестник Удмуртского университета. Серия «Экономика и право». 2024. № 4. С. 722-728.

10. Что такое «доксинг» и «сексторшен»: словарь цифрового насилия // Forbes Woman. URL: https://www.forbes.ru/forbes-woman/492411-cto-takoe-doksing-i-sekstorsen-slovar-cifrovogo-nasilia (дата обращения: 28.08.2025).

11. Шутова А. А. Анализ телемедицины на преступность: риски и тенденции, уголовно-правовое реагирование // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2022. № 4. С. 133-142. DOI 10.18384/2310-6794-2022-4-133-142. EDN УВОГСН.

УДК 342.2/7

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

Социальная инженерия как инструмент криминального цифрового воздействия

Аннотация. В настоящей статье проводится анализ трансформации социальной инженерии из тактики индивидуального психологического воздействия, применяемой в среде хакеров, как системный инструмент цифрового влияния на общественное сознание и политические процессы. Подчеркивается необходимость разработки комплексных, междисциплинарных мер противодействия, выходящих за рамки индивидуальной кибергигиены и охватывающих правовое регулирование и международное сотрудничество.

Ключевые слова: социальная инженерия, цифровая безопасность, претекстинг, дезинформация, манипуляция сознанием, цифровой суверенитет, цифровизация

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

Social engineering as a tool of criminal digital influence

Abstract. This article analyzes the transformation of social engineering from the tactics of individual psychological influence used among hackers into a systemic tool of digital influence on public consciousness and political processes. The need to develop comprehensive, interdisciplinary countermeasures that go beyond individual cyber hygiene and cover legal regulation and international cooperation is emphasized.

Keywords: social engineering, digital security, pretexting, disinformation, manipulation of consciousness, digital sovereignty, digitalization

Введение. Изначально термин «социальная инженерия» относился к противоправным практикам межличностного обмана, используемым для получения конфиденциальной информации путем психологического воздействия на отдельных лиц. В современных условиях данный феномен претерпел качественную трансформацию, став инструментом стратегического влияния на массовое сознание, способным дестабилизировать политические системы и подрывать доверие к демократическим институтам. Целью данного исследования является анализ методов социальной инженерии, а также выявление структурных факторов, обусловливающих ее эффективность в цифровую эпоху.

Основное содержание. Информационная глобализация и цифровизация, кардинально меняя общественные отношения, закономерно способствуют и трансформации преступности, порождая новые формы и инструменты противоправных посягательств. В сфере имущественных преступлений таким ключевым инструментом стала социальная инженерия. В своем исследовании Е.В. Зотина приходит к выводу о том, что социальная инженерия как главный инструмент мошенничества с использованием информационно-телекоммуникационных технологий, представляет собой криминальное манипулирование, заключающееся в целенаправленном воздействии преступника на эмоционально-волевую сторону жертвы посредством психолого-речевых приемов и осуществляемое в целях достижения преступной цели – хищения имущества либо приобретения права на чужое имущество путем обмана или злоупотребления доверием [2. С. 5].

Между тем, профессор А.Л. Осипенко отмечает, что методы социальной инженерии в большей степени выражаются в «предварительном сборе необходимой минимальной социальной информации о жертве; использование дистанционных технологий коммуникации, помогающих выдавать себя за другое лицо; использование при общении или переписке характерных выражений для имитации официальной беседы; упоминание различных известных фактов в совокупности с вымышленными; создания имиджа административно уполномоченного лица имеющего полномочия на запрашиваемую конфиденциальную информацию; выведение собеседника из состояния психического равновесия путем запугивания; использования резких выражений, понижающих самооценку собеседника; упоминание в разговоре важных знакомств и связей для формирования у жертвы состояния тревожности; запугивание жертвы возможностью наступления негативных последствий вследствие отказа предоставить запрашиваемую информацию; применение отдельных приемов для вхождения в доверии к жертве, использование лести, личного обаяния с целью установления дальнейшего психологического контакта» [3. С. 432].

Классическая модель социальной инженерии, описанная в работах Кевина Митника и Кристофера Хаднэги, включает четыре последовательных этапа: сбор информации (трэшинг), создание ложного контекста (претекстинг), установление контакта и манипуляция (буллшиттинг), а также непосредственная эксплуатация (пенетрация) [8].

Трэшинг, или разведка, исторически предполагал физический сбор отходов – документов, носителей информации – с целью получения данных о цели.

В цифровую эпоху данный этап полностью трансформировался: сбор информации осуществляется через открытые источники (OSINT), утечки баз данных, профили в социальных сетях и метаданные цифровых устройств. Современный «цифровой мусор» представляет собой ресурс, доступ к которому не требует физического присутствия, но обеспечивает исчерпывающую картину личности или организации [7, С. 158].

Претекстинг – конструирование правдоподобной лжи – изначально применялся в телефонных звонках, где злоумышленник представлялся сотрудником технической службы. В контексте массовых кампаний данный метод масштабируется: создаются тысячи фальшивых аккаунтов, имитирующих реальных пользователей с определенной идеологической повесткой.

Буллшиттинг, или распространение «чепухи», представляет собой не просто ложь, а принципиальное безразличие к истине. Его цель – не убеждение, а эмоциональная активация аудитории, провоцирование действий на основе страха, гнева или ненависти. Например, кампания Cambridge Analytica применяла психографические профили для доставки персонализированного контента, вызывающего эмоциональный отклик у конкретных категорий избирателей, что демонстрирует переход от массового воздействия к массперсональному [4, С. 22].

Компания получила доступ к персональным данным миллионов пользователей Facebook через стороннее приложение, что позволило построить детальные психографические профили. На их основе осуществлялась микротаргетированная доставка политических сообщений, адаптированных под индивидуальные страхи и предубеждения избирателей. В данном случае претекстинг осуществлялся на уровне отдельного пользователя, что повышало эффективность манипуляции [9. С. 23].

Приведенный кейс свидетельствует о том, что успех подобных кампаний определяется не технологическим превосходством, а глубоким пониманием социальной психологии, готовностью цифровых платформ быть использованными в качестве инструмента влияния и наличием предварительно существующих социальных разломов.

Ключевым фактором эффективности социальной инженерии является не индивидуальная уязвимость жертв, а структурная уязвимость общества. Успех хакера Кевина Митника объяснялся не актерским мастерством, а доверием его жертв к институциональным ролям и протоколам. Цифровая среда, благодаря своей анонимности, масштабируемости и алгоритмической персонализации, создает идеальные условия для реализации всех этапов социальной инженерии в промышленных масштабах. Социальные сети функционируют как платформы, автоматизирующие процессы сбора данных, создания контекста и распространения манипулятивного контента.

Следует обратить внимание на проведенный историко-теоретический анализ в исследовании И.Р. Бегишева и Д.Д. Берсей, который позволяет проследить трансформацию понятия «социальная инженерия» от социально-реформаторского инструмента к криминальному методу цифрового воздействия [1. С. 24-34]. Авторы подчеркивают, что термин изначально возник в социально-

экономическом дискурсе XIX века – у Т. Веблена и Дж. Аддамс – как обозначение рационального, научно обоснованного управления общественными процессами [5]. Однако уже к середине XX века, особенно в контексте Великой депрессии и «нового курса» Рузвельта, концепция приобрела черты прикладной дисциплины, ориентированной на «обуздание социальных приливов и отливов» [6. С. 245].

Ключевой поворот произошел с появлением цифровых технологий: социальная инженерия трансформировалась из инструмента социального планирования в метод манипуляции человеческим фактором с целью несанкционированного доступа к информации. И.Р. Бегишев и Д.Д. Берсей убедительно показывают, что эта эволюция не была случайной – она отражает смену парадигмы: от управления массами через институты к контролю над индивидами через их психологические уязвимости и цифровые следы. Авторы также акцентируют внимание на том, что современные социоинженерные атаки достигли уровня сложности, сопоставимого с техническими кибератаками, что требует пересмотра подходов к обеспечению информационной безопасности – с акцента на технологическую защиту – на комплексную защиту, включающую человеческий и организационный факторы [1. С. 28].

Соглашаясь с представленным суждением, следует подчеркнуть, что современная социальная инженерия представляет собой симптом цифровой эпохи, где личность становится ключевым объектом и одновременно уязвимым звеном в системе безопасности. Указанный фактор определяет ноеобходимость кардинального пересмотра стратегий защиты: не противопоставления технических и человеческих факторов, а их интеграции в единую систему, где устойчивость к манипуляциям формируется через осознание сотрудниками как ценности информации, так и механизмов собственного психологического воздействия.

Изучение практики показало, что социально-инженерные атаки реализуются через ряд последовательных стадий, направленных на манипуляцию человеческим фактором. Основными этапами данного процесса являются сбор информации, установление отношений и эксплуатация доверия.

На первом этапе осуществляется сбор информации, часто из открытых источников, таких как социальные сети. Публикуемые пользователями данные – персональные сведения, геолокация, профессиональные связи – формируют детальный профиль, который используется для дальнейшего целевого воздействия. Удаление такой информации затруднительно, что повышает ее ценность для злоумышленника.

Второй этап предполагает построение доверительных отношений с жертвой. Используя полученные ранее инсайдерские знания, злоумышленник создает иллюзию знакомства или общности интересов, эксплуатируя естественную склонность людей к доверию [11. С. 139].

На этапе эксплуатации осуществляется непосредственная манипуляция, направленная на достижение цели атаки – получение конфиденциальных данных или несанкционированного доступа. Атакующий использует эмоциональное состояние жертвы, побуждая ее к совершению определенных действий.

Таким образом, несмотря на возрастающую сложность социоинженерных атак, ключевым элементом защиты остается подготовленность пользователей, которые при должном уровне осведомленности способны эффективно противостоять манипуляциям.

Следует заключить, что традиционные меры кибербезопасности, ориентированные на индивидуальное поведение, оказываются неэффективными против системных кампаний массперсонального воздействия. Противодействие должно быть комплексным и включать следующие направления:

Во-первых, необходимо правовое регулирование цифровых платформ, включающее требования к прозрачности алгоритмов, борьбе с ботами и фейковыми аккаунтами, а также раскрытию источников финансирования политической рекламы. Саморегулирование в данном контексте доказало свою несостоятельность.

Во-вторых, требуется масштабная программа медиаграмотности, выходящая за рамки простых рекомендаций «не доверять всему в Интернете». Необходимо формирование у граждан навыков критического анализа информации, понимания механизмов манипуляции и распознавания тактик социальной инженерии.

В-третьих, следует развивать международное сотрудничество в области противодействия информационным вмешательствам. Угроза вмешательства в выборы носит транснациональный характер и требует выработки единых норм и механизмов ответственности [10. С. 12].

Заключение. Социальная инженерия в XXI веке трансформировалась из маргинальной практики в один из ключевых инструментов гибридных конфликтов. Ее методы – от сбора данных до распространения дезинформации – стали основой для кампаний, направленных на подрыв демократических институтов и манипуляцию общественным мнением. Понимание механизмов ее функционирования и структурных основ ее эффективности является необходимым условием для разработки адекватных мер противодействия. Будущее цифрового общества зависит от способности государств, институтов и граждан противостоять не только технологическим угрозам, но и манипуляции человеческим сознанием через эксплуатацию его социальных и когнитивных уязвимостей.

Список литературы

1. Бегишев И. Р., Берсей Д. Д. Генезис криминальной социальной инженерии // Цифровые технологии и право: Сборник научных трудов II Международной научно-практической конференции: в 6 томах, Казань, 22 сентября 2023 г. Казань: Издательство "Познание", 2023. С. 24-34.

2. Зотина Е. В. Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование: автореферат диссертации на соискание ученой степени кандидата юридических наук. Казань, 2025. 33 с.

3. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт. Москва: Юридическое издательство «Норма», 2021. С. 432.

4. AllahRakha N. Transformation of crimes (cybercrimes) in digital age //International Journal of Law and Policy. 2024. Т. 2. №. 2. P. 19-27.

5. Espinhara J., Albuquerque U. Using online activity as digital fingerprints to create a better spear phisher. Technical report, Trustwave SpiderLabs.

6. Griffiths D., Goddard T. An Explanatory Framework for Understanding Teachers Resistance to Adopting Educational Technology // Kybernetes. 2022. Vol. 44. P. 240-25

7. Dsouza D. S., Hajjar A. E., Jahankhani H. Deepfakes in social engineering attacks //Space Law Principles and Sustainable Measures. – Cham : Springer Nature Switzerland, 2024. P. 153-183.

8. Hicks R. Social Engineering: The Reliability of a Framed Social Engineering Acceptable Use Policy : дис. – Utica College, 2018.

9. Koza E., Öztürk A., Willer M. Definition: Social Engineering //Social Engineering und Human Hacking: Strategien zur Prävention und Abwehr von Manipulationstechniken in der IT. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2025. С. 19-27.

10. Maennel K., Maennel O. Human Aspects of Cyber Security for Computing Higher Education: Current Status and Future Directions //ACM Transactions on Computing Education. 2025. Т. 25. №. 3. С. 1-30.

11. Yuswanita A., Veri J. Pengaruh Human Error dan Sosial Engineering terhadap Tingkat Kebocoran Data pada Instansi Pemerintah //Indonesian Research Journal on Education. 2025. Т. 5. №. 5. С. 137–142.

УДК 343.988

Е. М. Глянц,
адвокат,
Коллегия адвокатов «Рыбак, Коган и партнеры»

Дети-сироты в цифровом пространстве: риски и стратегии виктимологической защиты

Аннотация. В настоящей статье исследуется актуальная проблема виктимизации детей-сирот в условиях цифровой трансформации общества. Автор анализирует специфические криминогенные факторы, обуславливающие повышенную уязвимость данной категории несовершеннолетних в виртуальной среде. Методологической основой исследования выступает комплексный виктимологический подход, позволяющий выявить корреляцию между социально-психологическими особенностями детей, оставшихся без попечения родителей, и их склонностью к виктимному поведению в киберпространстве. Особое внимание уделяется анализу механизмов криминального воздействия на несовершеннолетних через цифровые платформы, включая вовлечение в противоправную деятельность, кибербуллинг и сексуальную эксплуатацию. В работе предлагается концептуальная модель превентивного воздействия, основанная на принципах ранней диагностики виктимогенных ситуаций и внедрении комплексных защитных механизмов. Практическая значимость исследования заключается в разработке научно обоснованных рекомендаций по совершенствованию системы профилактики преступлений против детей-сирот в цифровой среде.

Ключевые слова: виктимология, дети-сироты, социальные сироты, цифровое пространство, киберпреступность, виктимизация, превенция, кибербезопасность, несовершеннолетние, виктимогенные факторы, цифровая защита

E. M. Glyants,
Advocate,
Bar association «Rybak, Kogan and partners»

Social portrait of an attack victim, based on social engineering methods

Abstract. This article examines the current problem of victimization of orphaned children in the context of digital transformation of society. The author analyzes the specific criminogenic factors that cause the increased vulnerability of this category of minors in a virtual environment. The methodological basis of the study is a comprehensive victimological approach that allows us to identify a correlation between the socio-psychological characteristics of children left without parental care and their tendency to victim behavior in cyberspace. Special attention is paid to the analysis of the mechanisms of criminal influence on minors through digital platforms, including involvement in illegal activities, cyberbullying and sexual exploitation. The

paper proposes a conceptual model of preventive action based on the principles of early diagnosis of victimogenic situations and the introduction of comprehensive protective mechanisms. The practical significance of the research lies in the development of scientifically based recommendations for improving the system of crime prevention against orphaned children in the digital environment.

Keywords: victimology, orphaned children, digital space, cybercrime, victimization, prevention, cybersecurity, minors, victimogenic factors, digital protection

Введение. Стремительная дигитализация социальных процессов актуализирует вопросы обеспечения безопасности наиболее уязвимых категорий населения в виртуальном пространстве [1]. «Современные технологии, Интернет и киберпространство изменили природу, типы и обстоятельства преступлений и преступников, а также инструменты контроля над ними. Новые формы преступности (например, киберпреступность) представляют более серьезную угрозу и опасность для всех слоев общества» [2. С. 243]. Дети-сироты и дети, оставшиеся без попечения родителей, находясь в состоянии социальной дезадаптации, демонстрируют повышенную подверженность виктимизации в условиях цифровой среды. Данное обстоятельство обуславливает необходимость переосмысления традиционных подходов к виктимологической профилактике с учетом специфики киберпространства.

Современная доктрина уголовно-правовой науки рассматривает виктимность как сложный социально-психологический феномен, детерминирующий вероятность причинения вреда определенным категориям граждан [3]. В контексте цифровой трансформации общества данная концепция приобретает принципиально новые измерения, требующие глубокого научного осмысления.

Основная часть. Анализ криминологической обстановки в киберпространстве свидетельствует о формировании специфических условий, способствующих виктимизации несовершеннолетних [4]. Дети-сироты и дети, оставшиеся без попечения родителей, в силу своих психосоциальных характеристик обладают повышенной восприимчивостью к криминогенному воздействию виртуальной среды.

Первостепенное значение имеет феномен псевдоанонимности цифрового пространства, создающий иллюзию безнаказанности у потенциальных субъектов преступлений. Данное обстоятельство способствует активизации криминальных элементов, специализирующихся на совершении преступлений против несовершеннолетних. Особую опасность представляют лица, использующие методы социальной инженерии для установления доверительных отношений с детьми-сиротами.

Дефицит социального контроля в цифровой среде создает благоприятную почву для манипулятивного воздействия на несовершеннолетних. Дети-сироты, испытывающие острую потребность в эмоциональной поддержке и признании, становятся легкой мишенью для злоумышленников, эксплуатирующих их психологические особенности.

Систематизация эмпирического материала позволяет выделить основные модели виктимного поведения детей-сирот в цифровой среде. Наиболее распро-

страненной формой является неосторожное раскрытие персональной информации в социальных сетях и мессенджерах. Данное поведение обусловлено недостаточным уровнем цифровой грамотности и отсутствием адекватных защитных механизмов [5].

Значительную долю составляют случаи вовлечения несовершеннолетних в противоправную деятельность через игровые платформы и специализированные онлайн-сообщества. Криминальные структуры целенаправленно используют психологические особенности детей-сирот, предлагая им иллюзорные возможности социальной интеграции и материального благополучия.

Отдельного внимания заслуживает проблема кибербуллинга, жертвами которого преимущественно становятся дети с нарушенными социальными связями. Систематическое психологическое воздействие в виртуальной среде может привести к серьезным деформациям личности и формированию устойчивых виктимных установок.

Современные технологии предоставляют злоумышленникам широкий арсенал средств для осуществления криминального воздействия на несовершеннолетних [6]. Особую опасность представляет использование алгоритмов машинного обучения для идентификации потенциальных жертв на основе анализа их цифрового следа.

Преступники активно эксплуатируют геймификационные механизмы для постепенного вовлечения детей в противоправную деятельность. Данный подход позволяет нивелировать естественные психологические барьеры и сформировать у несовершеннолетних ложное представление о безопасности совершаемых действий.

Криптографические технологии, изначально созданные для защиты информации, парадоксальным образом становятся инструментом сокрытия преступной деятельности. Использование анонимных мессенджеров и криптовалют существенно затрудняет выявление и расследование преступлений против детей-сирот в виртуальном пространстве.

Разработка эффективной системы защиты детей-сирот в киберпространстве требует комплексного подхода, основанного на принципах превентивного воздействия и ранней диагностики виктимогенных ситуаций. Ключевым элементом данной системы должна стать цифровая грамотность как основа формирования защитного поведения.

Принципиальное значение имеет создание специализированных алгоритмов мониторинга цифровой активности детей-сирот и детей, оставшихся без попечения родителей, с целью своевременного выявления признаков виктимизации. Данные системы должны базироваться на машинном обучении и анализе поведенческих паттернов, характерных для ситуаций повышенного риска.

Необходимо развитие института цифрового наставничества, предполагающего персонализированное сопровождение детей-сирот в процессе освоения виртуального пространства. Такой подход позволит обеспечить индивидуализированную профилактику с учетом специфических потребностей каждого ребенка.

Модернизация системы виктимологической защиты должна осуществляться по нескольким взаимосвязанным направлениям. Первостепенное значе-

ние имеет совершенствование нормативно-правовой базы, регулирующей вопросы безопасности детей в цифровой среде. Необходимо устранить существующие правовые лакуны и обеспечить адекватную криминализацию новых форм преступного поведения.

Техническая составляющая защитных механизмов должна включать разработку специализированного программного обеспечения для контроля цифровой активности детей-сирот. Данные системы должны обеспечивать баланс между защитой и сохранением права несовершеннолетних на приватность.

Образовательный компонент предполагает внедрение специализированных программ повышения цифровой грамотности, адаптированных с учетом психологических особенностей детей, оставшихся без попечения родителей. Особое внимание должно уделяться формированию критического мышления и навыков распознавания манипулятивных техник.

Заключение. Проведенное исследование позволяет сделать вывод о необходимости кардинального переосмысления подходов к обеспечению безопасности детей-сирот и детей, оставшихся без попечения родителей, в условиях цифровой трансформации общества. Традиционные методы виктимологической профилактики требуют существенной модификации с учетом специфики киберпространства.

Эффективная защита детей-сирот в цифровой среде возможна лишь при условии комплексного подхода, включающего правовые, технические, образовательные и психологические компоненты. Ключевое значение имеет своевременная идентификация виктимогенных ситуаций и внедрение превентивных механизмов воздействия.

Дальнейшее развитие исследований в данной области должно быть направлено на разработку практических инструментов диагностики и профилактики виктимизации детей-сирот в киберпространстве. Междисциплинарный характер проблемы обуславливает необходимость интеграции достижений криминологии, виктимологии, психологии и информационных технологий.

Список литературы

1. Майоров А. В. Виктимология цифровой преступности: концепция научного направления // Виктимология. 2024. Т. 11, № 1. С. 7-12. EDN ZRALDW.

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

3. Пинкевич Т. В., Нынюк Р.Н. Виктимизация несовершеннолетних от насильственных преступлений сексуального характера в условиях цифровизации: детерминация и предупреждение // Всероссийский криминологический журнал. 2024. Т. 18, № 2. С. 149-159. EDN OMBOJA.

4. Родина Е. А. Виктимологическое предупреждение преступлений в киберпространстве // Актуальные проблемы государства и права. 2021. Т. 5, № 19. С. 510-524. EDN VSELXO.

5. Фоминых Е. С. Нарушения информационной безопасности в контексте цифровой виктимизации детей и подростков // Виктимология. 2024. Т. 11, № 1. С. 69-77. EDN AUDIJK.

6. Шайкова М. В. Характеристика виктимологического поведения несовершеннолетних в социальных сетях // Защита жертв преступлений в современном обществе (PVCMS 2024) : Сборник материалов VII Международной научно-практической интернет-конференции, Челябинск, 21–22 февраля 2024 года. Челябинск: ООО «Эскуэла», 2024. С. 90-99. EDN HWBEBG.

УДК 340, 342

Н. Л. Денисов
кандидат юридических наук, доцент
Московский государственный юридический университет,
имени О. Е. Кутафина (МГЮА)

Концепция государственного регулирования цифрового мира

Аннотация. В современный цифровой мир погружается все больше и больше людей, кроме того он развивается и усовершенствуется, постепенно копируя и реализуя возможности реального мира. Эти возможности как положительные, так отрицательные. В частности, участникам данного мира грозят реальные имущественные и другие проблемы. Однако, к сожалению, государство не принимает должного участия в регуляции данных отношений, ограничиваясь исключительно регламентированием отдельных проявлений цифровой активности граждан, которое не имеет общей концепции. В рамках данной статьи данная концепция была предложена.

Ключевые слова: цифровой мир, метавселенная, государственное регулирование, киберпреступность, альтернатива реального мира, онлайн-игры, образования цифрового мира

N. L. Denisov,
Candidate of Law,
Associate Professor O.E. Kutafin Moscow State Law University

The concept of state regulation of the digital world

Abstract. More and more people are immersed in the modern digital world. Furthermore, it is developing and improving, gradually copying and implementing the capabilities of the real world. These capabilities are both positive and negative. In particular, participants in this world face real property and other problems. However, unfortunately, the state does not play a proper role in regulating these relations, limiting itself solely to regulating individual manifestations of citizens' digital activity, which lacks a general concept. This article proposes such a concept.

Keywords: digital world, metaverse, state regulation, cybercrime, alternative real world, online games, digital world formations

Введение. В настоящее время цифровой мир становиться все более значимым в жизни людей. Эта значимость определяет не только помощь в поиске информации и обеспечение удобной связи, но все большим погружением значительного числа людей. Погружение может выражаться как в формировании увлеченности компьютерными играми и другими образованиями цифрового мира, приобретения и реализация себя в хобби опять-таки в рамках образований цифрового мира, поиске друзей и формирование социальной группы по-

средством сетей и других образований цифрового мира, и, наконец, увеличивается число людей, которые предпочитают создавать и (или) участвовать в онлайн симуляторах реальной жизни (например, метавселенные). И дальше погружение будет еще больше, особенно с развитием и доступностью технологий виртуальной реальности, реалистичности и функционала образований цифрового мира.

Основная часть. С увеличением погружения и количества погруженных происходит изменения роли и значимости для государства, общества и отдельных личностей цифрового мира.

Следует отметить, что до сих пор участие людей в образованиях цифрового мира рассматривается частью населения и государственными органами как забава, типа как детский сад, на который не следует обращать внимание. Однако это в настоящее время уже не так. Сейчас указанное участие для значительного числа людей стало намного большим, чем просто средство досуга.

Образования цифрового мира и сопутствующие элементы таких образований стали для людей альтернативой реального мира или как минимум его существенным дополнением.

В частности, возникли в данных образованиях отношения по выполнению каких-либо работ, оказанию услуг, купли-продажи (в том числе и за реальные деньги). Однако наиболее важным является то, что в них люди нашли способ реализоваться, найти себя как личности.

Соответственно, если в них возникают проблемы или (и) споры, то это оказывает существенное влияние на людей, на их психическое, эмоциональное состояние.

Все это является основанием для того, что начать воспринимать деятельность образований цифрового мира и взаимодействие в них участников как новую сферу социальных отношений с вытекающей необходимостью государственного контроля и регулирования.

В частности, раз идет речь о значимости для личности реализации в данных образованиях, то это уже предполагает официальную защиту государством.

Можно выделить следующие виды образований цифрового мира.

По степени реализации интересов можно условно определить назначение:

– для полной симуляции жизни (метавселенные), характеризуется полной альтернативой реального мира;

– учебных целей (для обучения), они создаются, как правило, в виде онлайн аудиторий;

– досуга (онлайн игры), создаются по мотивам или на основе определенных игр и представляют собой искусственный игровой мир;

– общения (дарк нет), создаются места для общения, которые предполагают значительные возможности для анонимности и связаны, как правило, с общением и сделками;

– производственных целей (в рамках предприятия), включают в себя имитацию определенных технических и (или) технологических процессов.

Данный перечень не полный. Со временем оно может расширяться.

По внутренней экономике следует различать:

– без использования каких-либо платежей, в таких образованиях нет ни игровой, ни возможности покупки за реальную валюту;

– с использованием внутренних платежей, вводится игровая, внутренняя валюта, однако покупки за реальные деньги не предусмотрена.

– с двойной системой платежей, в этих образованиях можно приобретать игровое имущество и бонусы как за игровую валюту, так и за реальные деньги;

По степени индивидуализации личности:

– без индивидуализации, идентификация участников осуществляется исключительно по никам;

– условной индивидуализацией, в таких образованиях пользователям предоставляется возможность выбрать либо случайные аватарки, либо или аватарки сказочных (игровых) героев;

– частичной индивидуализацией, при регистрации пользователь изначально настраивает свой виртуальный образ;

– полной индивидуализации, в таких образованиях можно установить или отсканировать свое фото.

Говоря об указанных видах, следует отметить, что на использование реальных денег и полной индивидуализации необходимо особый контроль государства (выдача лицензий и т. д.), так как в этом случае имеется возможность причинения реального вреда гражданам.

Кроме того для отдельных категорий ввести основы функционирования образования цифрового мира (минимальный свод правил), а также арбитраж (для решения споров), куда включить представителей создателей образований, чиновников аппарата и представителей общественности (это на далекую перспективу, а пока можно создать комиссию в рамках министерства цифрового развития, связи и массовых коммуникаций Российской Федерации).

Заключение. В целом в настоящее время возможно частичное решение вопросов путем создания отдельного ведомства, которое будет заниматься вопросами участия государства в регулирования отношений в цифровом мире, введя в его структуру исследовательский центр, который будет заниматься изучением данного мира и отношений в нем.

УДК 343.34

Г. К. Джамбулатов,
Управление МВД России
по городу Екатеринбургу

Виктимологические аспекты профилактики преступлений во время публичных массовых мероприятий

Аннотация. В статье рассматриваются отдельные вопросы виктимологической профилактики во время публичных массовых мероприятий (включая протестные акции). Обозначены распространенные детерминанты преступлений, совершаемых в период проведения публичных массовых мероприятий. Обращено внимание на вопросы виктимологической безопасности участников публичных массовых мероприятий, а также сотрудников органов внутренних дел и Росгвардии, задействованных в несении службы по охране общественного порядка и общественной безопасности вовремя и на месте проведения публичных массовых мероприятий. Приводится перечень виктимогенных ситуаций, которые возникают в деятельности сотрудников полиции. Предложены меры виктимологической профилактики преступлений, совершаемых во время публичных массовых мероприятий.

Ключевые слова: публичные массовые мероприятия, протестные акции, предупреждение преступлений, полиция, Росгвардия, виктимологическая безопасность, виктимологические ситуации, виктимологическая профилактика

G.K Dzhambulatov,
Department of the Russian Ministry of Internal Affairs
for the City of Yekaterinburg

Victimological aspects of crime prevention during public events

Abstract. The article discusses certain issues of victimological prevention during public mass events (including protests). It identifies common determinants of crimes committed during public mass events. The article focuses on the victimological safety of participants in public mass events, as well as employees of the Ministry of Internal Affairs and the National Guard, who are involved in maintaining public order and security during and at the site of public mass events. The article provides a list of victimogenic situations that arise in the work of police officers. Victimological prevention measures for crimes committed during public mass events have been proposed.

Keywords: public mass events, protests, crime prevention, police, Russian National Guard, victimological security, victimological situations, victimological prevention

Введение. Исследование вопросов криминологического предупреждения преступлений, совершаемых в период проведения публичных массовых мероприятий, наглядно показало, что данная проблематика в науках уголовно-правового цикла в современный период остается актуальной и потому недостаточно исследованной [1]. В этой связи отдельного внимания от криминологов требуют виктимологические аспекты профилактики преступлений во время публичных массовых мероприятий, поскольку «вместе с традиционной профилактикой виктимологическая делает предупредительную деятельность логически завершенной» [4]. Нельзя также не отметить, что виктимологическая профилактика анализируемых преступлений, как нам представляется верным, является перспективным и востребованным этапом всей предупредительной деятельности, наряду с предотвращением, пресечением преступлений.

Основная часть. Виктимологическая безопасность организаторов и участников публичных массовых мероприятий, а также сотрудников органов внутренних дел, Росгвардии, задействованных в несении службы по охране общественного порядка и общественной безопасности вовремя и на месте проведения публичных массовых мероприятий, можно рассматривать как важнейший аспект системы предупреждения преступлений, совершаемых в период проведения публичных массовых мероприятий [1].

Среди жертв преступлений – участников публичных массовых мероприятий (включая протестные акции) ранее было предложено выделить три типа [1]: случайные жертвы; ситуативные жертвы и профессиональные жертвы.

Выделение профессиональной жертвы преступлений – участников публичных массовых мероприятий и, выработка оптимальных мер виктимологической профилактики преступлений обусловлена практической потребностью минимизации жертв анализируемых преступлений и повышения престижа органов внутренних дел [5].

Повышенная виктимность обусловлена видом их профессионально-служебной деятельности, связанной практически беспрерывной занятостью, отсутствием свободного времени, работой в ночное время, в выходные и праздничные дни, необходимостью реализации требований в ограниченные промежутки времени [7. С. 44]. Сотрудник ориентируется на навязанный ритм и отвлекается от своих запланированных дел, связанных с личными делами или же выполнением обязанностей родителя, законного представителя. Привлечение к несению службы во время несогласованной протестной акции может сопровождаться психоэмоциональным напряжением, раздражительностью и эмоциональным расстройством. Как показывает практика и личный опыт службы в ОВД автора настоящего исследования в условиях дефицита личного времени у сотрудников полиции, склонных к распитию спиртных напитков, выставление последних в выходные дни для охраны общественного порядка во время многотысячного несогласованного, стихийного митинга может сопровождаться психоэмоциональным напряжением, раздражительностью и эмоциональным расстройством [1].

По мнению А. В. Маргачевой, «одним из наиболее важных аспектов обеспечения виктимологической безопасности, является выявление виктимогенных

(виктимообразующих) ситуаций, в рамках которых проявляется профессиональная виктимность» [8. С. 278-279].

Согласимся с исследователями, которые обращают внимание на роль виктимогенных ситуаций, которые возникают в деятельности сотрудников полиции, связанных:

1) с провокационными действиями сотрудников полиции;

2) их возможными незаконными действиями;

3) тактически неправильными действиями сотрудников полиции;

4) психологически безграмотным поведением сотрудников полиции в конкретной ситуации [2, С. 35, 3. С. 11].

Заключение. Подводя небольшой итог исследованию, следует отметить следующее. Любое публичное массовое мероприятие сопровождается рисками совершения тяжких преступлений в отношении сотрудников органов правопорядка, что в условиях нарастания дефицита профессиональных кадров в органах внутренних дел России, недопустимо.

В качестве виктимологических мер профилактики преступлений, совершаемых во время публичных массовых мероприятий можно выделить: еженедельное проведение занятий с личным составом по тактике пресечения и локализации противоправных действий со стороны участников протестных акций, «гражданских активистов», представителей экстремистских и террористических организаций; регулярные теоретические занятия по анализу практики привлечения лиц к административной ответственности за совершение правонарушений во время и на месте проведения публичных массовых мероприятий (включая протестные акции) сотрудников подразделений по исполнению административного законодательства, подразделений по делам несовершеннолетних, подразделений по предотвращению преступлений во время массовых и спортивных мероприятий, подразделений по организации борьбы с противоправным использованием информационно-коммуникационных технологий, специальных подразделений для обеспечения безопасности и правопорядка в сфере эксплуатации беспилотных летательных аппаратов и подразделений по охране общественного порядка.

Список литературы

1. Джамбулатов Г. К. Виктимологическая характеристика личности жертвы преступления–участника публичных массовых мероприятий // Виктимология. 2024. Т. 11, №1 С. 132–143. DOI: 10.47475/2411-0590-2024-11-1-132-143.

2. Дубровина М.В. Профессиональная виктимность сотрудников органов внутренних дел // Защита жертв преступлений в современном обществе (PCVMS 2024): материалы VII Международной научно-практической интернет-конференции (Челябинск, 21-22 февраля 2024 г.). Отв. ред. А.В. Майоров. Челябинск: Эскуэла, 2024. С.11. URL: https:// victimolog.ru/ index.php/ PVCMS /article /view/628.

3. Гарманов, В.М. Отдельные направления предупреждения виктимности сотрудников полиции // Виктимология. 2014. № (2). С. 34-40.

4. Криминология: Учебник для вузов / под общ. ред. д. ю. н., проф. А. И. Долговой. 3-е изд., перераб. и доп. М.: Норма, 1997. 784 с.

5. Маджумаев М.М. Уголовная ответственность за массовые беспорядки в Соединенных штатах Америки: автореф. дис…канд. юрид. наук. Москва. 2022.

6. Маргачева А.В. Криминологическая оценка виктимологической безопасности органов внутренних дел при пресечении незаконных публичных мероприятий // Уголовная политика и культура противодействия преступности : материалы Междунар. науч.-практ. конф., 24 сент. 2021 г. / редкол.: А. Л. Осипенко, К. В. Вишневецкий, В. С. Соловьев и др. Краснодар : Краснодарский университет МВД России, 2021. С. 278-279

7. Рябова М.Г., Канунников Р.И. Личностные детерминанты форм аддиктивного поведения у сотрудников органов внутренних дел (на примере ургентной зависимости) // Психология и право. 2022. Т. 12, № 1. С. 44–53 . DOI: https://doi .org/10 .17759/psylaw .2022120104.

8. Global Protest Tracker. Data updated on March 4, 2022. Carnegie Endowment for International Peace https://carnegieendowment.org /publications /interactive/protest-tracker (20.07.2025).

УДК 343.9

Е. И. Думанская,
кандидат юридических наук, доцент
Уральский государственный юридический университет
имени В. Ф. Яковлева,
Уральский государственный университет путей сообщения

Тенденции криминологического и виктимологического прогнозирования в условиях цифровизации

Аннотация. Статья посвящена тенденциям в криминологическом и виктимологическом прогнозировании в связи с возможностями внедрения искусственного интеллекта, информационных технологий. Рассматривается математическое моделирование для повышения эффективности оценок рисков рецидива, что позволит вырабатывать стратегии предупреждения индивидуального преступного поведения. Рассматриваются предложения количественно описывать индивидуальное поведение человека перед совершением и в момент преступления путем построения математической модели в виде интегрального уравнения и решения задачи численными методами.

Ключевые слова: цифровизация, криминологическое прогнозирование, виктимологическое прогнозирование, математическая модель, рецидив, оценка риска, профилактика

E. I. Dumanskaya,
candidate of juridical sciences, associate professor,
Ural State Law University named after V. F. Yakovlev,
Ural State University of Railway Transport

Criminological and victimological prediction trends in the digitalization

Abstract. The article speaks about some criminological and victimological prediction trends using artificial intelligence and information technologies. The mathematical modeling allows to improve the recidivism risks assessments. This makes it possible to develop the prevention of personal criminal behavior. The article focuses on the description of an individual's behavior before and during a crime by numerical methods using mathematical model in the form of an integral equation

Keywords: digitalization, criminological prediction, victimological prediction, mathematical model, relapse, risk assessment, prevention

Введение. Бурное развитие информационных и цифровых технологий требуют от криминологической науки совершенствования методологии исследования. В частности, внедрение искусственного интеллекта, в том числе в социальные сферы, ставит вопросы реализации новых возможностей криминологического прогнозирования. С учетом этих вызовов требуют переосмысления

результаты предшествующих отечественных исследований в этой области, так как использование цифровой и математической обработки криминологической информации позволяет увеличить точность прогнозных оценок. А масштабное внедрение цифровизации позволяет более активно использовать прогностические функции в теории и практике противодействия преступности.

В этой связи особо актуальными является предупреждение индивидуального преступного поведения, оценка риска рецидива и разработка научно обоснованных рекомендаций для его прогнозирования. Важным направлением развития для целей профилактики преступного поведения представляется, в том числе, криминологическое прогнозирование вероятности совершения индивидом преступления. Также актуальным в цифровую эпоху становятся вопросы виктимологического прогнозирования, особенно в контексте увеличения киберпреступлений.

Основная часть. Вопросы криминологического прогнозирования традиционно рассматривались учеными через призму системы инструментов эффективного управления или сдерживания преступности. Несмотря на огромную значимость данной криминологической категории, указанное направление долгое время являлось одним из наименее разработанных. Если в США разработки в сфере краткосрочного прогнозирования уже около 10 лет являются практическим инструментом деятельности территориальных подразделений полиции (в основном в крупных городах), то в России остаются в рамках исключительно научных исследований [6. С. 147].

Обращаясь к истокам отечественной школя прогнозирования, следует упомянуть одну из первых монографических работ, опубликованной в 1972 г. Г. А. Аванесовым «Теория и методология криминологического прогнозирования», которая, «по-прежнему, не теряет своей актуальности, а, наоборот, с каждым годом все больше приобретает практическую значимость» [2. С. 10]. Ученый писал, что прогнозирование — это «. . . своеобразный инструмент, с помощью которого можно составить оптимальный и эффективный перспективный план, направленный на то, чтобы система мер борьбы с преступностью (цели, средства, методы и т.д.) и ее внутренняя координация соответствовали интересам и потребностям не только настоящего, но и будущего» [1. С. 4]. Среди прогнозов можно выделить научное предвидение динамики и структуры преступности в целом, прогноз развития факторов, детерминирующих преступность, прогнозирование индивидуального антиобщественного поведения. При прогнозировании осуществляется анализ статистических данных за предыдущий период, выявляются закономерности преступности, которые переносятся на будущий период. При таком линейном экстраполировании возможно получить данные о предполагаемых изменениях преступности на коротких временных промежутках (до года) [11]. Безусловно, уже в тот период времени в качестве условий эффективности прогнозирования рассматривалось использование достоверных и полных статистических данных с использованием возможностей электронно-вычислительных машин.

Криминологическое прогнозирование отличается множественностью и разнообразием объектов исследования, к которым относятся: «. . . преступность,

ее отдельные формы и виды, наиболее вероятные варианты развития криминологической ситуации, ожидаемый социальный образ наиболее опасного преступника, социальный портрет жертвы, индивидуальное преступное поведение, сама криминологическая наука» [7. С. 76].

Для решения выше указанных задач используются различные методы и подходы. В литературе даже предлагается концепция криминологической футурологии как области исследований, которая занимается прогнозированием тенденций и возможных состояний преступности и «стремится понять, насколько различные факторы способны повлиять на содержание преступности в будущем, изменять формы и методики совершения криминальных деяний и, соответственно, подходы к их предотвращению» [10. С. 134]. Однако, в данной работе нам бы хотелось сосредоточится на возможностях методов математического прогнозирования и сферы их применения в области изучения преступного поведения.

В настоящее время математические модели стали широко использоваться в различных не только технических науках, но и в экономике, медицине, биологии, а также в гуманитарных науках. Значительно меньше публикаций с использованием математических моделей встречается в зарубежной правовой науке [18, 24]. Предлагаются различные способы оценки рисков рецидива, которые могут помочь судьям при вынесении приговора [19, 20]. Строятся прогностические модели [14], используются математические методы обработки статистической информации [17] и корреляционный анализ.

Также отечественные современные исследования сосредотачиваются на использовании пространственных и пространственно-временных моделей, а также методов искусственного интеллекта, выделяя различные экономические, социальные, географические, временные и другие группы факторов, оказывающие влияние на состояние преступности [13. С. 123]. При этом используемые различные методы статистического анализа не являются какими-то новыми. Например, картирование преступности используется правоохранительными органами уже достаточно продолжительное время [См. 5]. Также в литературе встречается криминологическое прогнозирование на основе тренда при недостаточной точности описания моделью исходных данных [8].

Существуют и вероятностные прогностические подходы к оценкам риска рецидива [23]. Прогнозирование индивидуального преступного поведения личности представляет собой исключительную сложную задачу [22].

Обозначенные выше, а также иные подходы ставят криминологию на путь цифровизации, высказываются идеи об алгоритмической криминологии и вычислительнай криминологии, включающей в себя прикладную математику, то есть компьютерное моделирование преступного поведения. С помощью математики и информатики криминологические теории оживают и помогают объяснить преступность и работу правоохранительных органов [3. С. 242].

Как уже было отмечено выше, с учетом развития цифровизации и использования возможностей искусственного интеллекта, представляет интерес самая наименее разработанная категория криминологического прогнозирования – прогнозирование индивидуального преступного поведения.

В наше время всеобщей цифровизации, проникающей во все сферы нашей жизни (высокопроизводительные компьютеры, различных регистрирующие средства, искусственный интеллект и т.д.), по-видимому, можно приступить к созданию математических моделей, позволяющих описывать негативное поведения человека склонного к правонарушению. Такие модели позволят, прогнозировать поведение личности, склонной к правонарушению и оценивать опасность этой личности относительно других личностей, совершивших правонарушение.

При криминологическом прогнозировании перед исследователями стоит задача формализации и учета очень широкого спектра факторов. Это и экономические (безработица, уровень доходов населения, его покупательная способность), и социальные (миграция, урбанизация и плотность населения), и медицинские (распространенность алкоголизма и наркомании), и политические (эффективность государственного управления и судебной системы, уровень коррупции) вплоть до территориальных и временных факторов (освещенность улиц и наличие камер видеонаблюдения, географическое положение, особенности инфраструктуры). Необходимо также учитывать психологические и личностные факторы и виктимологические характеристики.

При индивидуальном криминологическом прогнозировании в качестве факторов, детерминирующих преступное поведение, на базе анализа которых происходит моделирование, обычно выделяют: жизненный опыт личности (наличие судимостей, прошлое противоправное и аморальное поведение), социальные ценности и ориентации, психофизиологические особенности, мотивы поведения (в том числе неосознаваемые установки и паттерны поведения), наличие образования, профессиональная принадлежность, социальные контакты, связи с маргинальными группами, влияние среды: социальной, микросоциальной, семейной, малых групп, а также возможность изменения личностных особенностей и социальных связей и факторов, которые могут детерминировать данные изменения» [4. С. 119].

Представляется, что совершенствование технологий и методик прогнозирования со временем позволит моделировать не только прогноз поведения личности, но и прогноз эффективности профилактического воздействия. Необходимо оценивать вероятность изменения ценностных ориентаций, потенциал к исправлению, социальной адаптации индивида.

На современном этапе трудности при прогнозировании индивидуального преступного поведения вызваны, во-первых, множеством факторов (внешних, внутренних), обуславливающих поведение человека. Мы не можем формализовать и охватить их в полном объеме, а также отсутствует полное понимание причинно-следственных связей конкретного фактора для конкретного человека. Во-вторых, отсутствуют универсальные критерии определения опасности личности и склонности к преступлению. Криминологически значимые признаки сложно описать математически и измерить.

Предсказание вероятности совершения преступления конкретным лицом должно включать разработку методики прогнозирования, базирующуюся на технологиях обработки больших данных. Функции оценки рисков, выполняе-

мые человеком, «все чаще дополняются рядом актуарных, алгоритмических инструментов и искусственного интеллекта, которые призваны обеспечивать точные возможности прогнозирования просоциального или преступного поведения и в этом случае основу прогноза составляют эмпирически определенные факторы риска (например, возраст, количество преступлений, проблемы в детстве, семье и т. д.), которые связаны с преступным поведением посредством статистически значимой взаимосвязи» [5. С. 55].

Представляется, что общую междисциплинарную задачу по созданию математической модели девиантного поведения человека можно представить, как:

1) задачу математической формализации действующих законодательных и моральных принципов, существующих в обществе;

2) задачу разработки математической модели в виде интегрального уравнения, которое описывает функцию опасности личности с учетом тяжести совершенного правонарушения;

3) задачу прогнозирования негативного поведения личности на основе экстраполяции социальных детерминант, влияющих на личность.

В связи с этим в ряде исследований [15, 16] предлагается количественно описывать индивидуальное поведение человека перед совершением и в момент преступления. Данная модель базируется на посылке, что на поведение индивидуума влияет множество негативных действующих факторов, приводящих к правонарушению, которые формализованы в некоторой системе множеств. Индивидуальное поведение может быть формализовано на основе простых правил суммирования независимых компонент, негативно влияющих на личность (например, социальная деградация, маргинализация, алкоголизация, наркотизация, наличие судимостей и т. д.). Также учитываются негативные социальные факторы, которые известным способом коррелируют с общей преступностью (например, международная миграция, дефицит денежного дохода, численность безработных, урбанизация). Модель основана на гипотезе, что вероятность совершения преступления личностью, описывается законом распределения дискретной вероятности совершения преступления в некотором заданном временном периоде. Данная гипотеза позволяет записать уравнение, в котором неизвестным является опасность личности. Дискретизация по времени некоторого периода наблюдения за личностью позволяет полученное интегральное уравнение свести к линейным алгебраическим уравнениям, которые могу быть легко решены. И чем больше факторов, характеризующих негативные социальные процессы, негативные личностные черты, способствующие совершению преступлений, включая мотивы, в том числе не осознаваемые будут учтены в модели, чем меньше интервалы времени будут взяты для наблюдения, тем достоверней будет показатель опасности личности, необходимый для прогноза.

Еще одним вызовом в условиях цифровизации становится разработка методик виктимологического прогнозирования. Задачей виктимологического прогнозирования является «изучение процесса виктимологического противодействия преступности в условиях снижения виктимности отдельных лиц и виктимизации общества» [12. С. 54]. Виктимологическое моделирование, отражающее детерминанты виктимности и виктимизации, позволит распознать тенден-

ции и логику развития прогнозируемого процесса, что способствует эффективному распределению сил и ресурсов для реагирования и работы с потенциальными и реальными жертвами.

Результатами совершенствования методов виктимологического и криминологического прогнозирования могут выступать повышение эффективности ведения информационно-аналитической деятельности, принятия различных управленческих решений, разработки специальных профилактических мероприятий для различных целевых групп, включая социальную поддержку и ситуативную профилактику. В контексте прогнозов индивидуального преступного поведения такое прогнозирование дает возможность планировать и применять профилактические меры воздействия, снижая риск повторных правонарушений.

Безусловно, поставленные выше задачи требуют внедрения программных комплексов и аналитических систем, основанных на новых цифровых технологиях и искусственном интеллекте. Разработка инструментов криминологического и виктимологического прогнозирования и оценки рисков должна осуществляться при использовании достаточно больших репрезентативных выборок и надежного статистического моделирования. Методики оценки рисков, особенно при индивидуальном прогнозировании, должны регулярно обновляться и уточняться на основе текущих данных, данных мониторинга, а не базироваться на единовременных статистических данных.

Заключение. Цифровизация все больше и больше проникает во многие отрасли науки, в том числе в гуманитарные и социальные науки. Однако, необходимо помнить, что это использование определенных алгоритмов ставит перед исследователями сложные вопросы и задачи.

Даже если смоделированная оценка риска будет правильно предсказывать рецидив, само по себе это не подразумевает эффективности профилактического воздействия. Даже если существует возможность воздействовать на факторы риска. Возникает проблема прогнозирования эффектов профилактического воздействия, что невозможно сделать без выявления причинно-следственных механизмов как факторов риска, так и факторов профилактического воздействия и их взаимосвязей.

В заключение необходимо отметить, что любая методика прогнозирования должна подвергаться постоянной переоценке сообразно с текущими вызовами, а также беспристрастной проверке.

Список литературы

1. Аванесов Г. А. Криминологическое прогнозирование и планирование борьбы с преступностью М., 1972, 60 с.

2. Антонян Ю. М. Профессор Г. А. Аванесов, классик отечественной криминологии // Криминологический журнал. 2022. № 4. С. 9-14. URL: https://doi.org/10.24412/2687-0185-2022-4-9-14.

3. Асли М. Р. Цифровые тренды криминологии и уголовного правосудия XXI века // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 235-250. URL: https://doi.org/10.21202/jdtl.2023.9.

4. Афанасьева О. Р., Глеба О. В. Криминологическое прогнозирование индивидуального преступного поведения // Международный научно-исследовательский журнал. 2017. № 3-2 (57). С. 118-121.

5. Батоев В. Б. О картировании преступности и предиктивной аналитике в оперативно розыскной деятельности // Правопорядок: история, теория, практика. 2023. № 2 (37). С. 134-139.

6. Бондарева Г. В. Понятие и современное состояние криминологического прогнозирования // Философия права. 2022. № 4 (103).,147-151

7. Буранова Р. Е. Криминологические прогнозы преступности и их типы // EURASIAN JOURNAL OF ACADEMIC RESEARCH. 2024. Vol. 4, Iss. 1, P. 2. Pp.76-87

8. Деменченок О. Г., Баранов С. А. Криминологическое прогнозирование на основе тренда при недостаточном качестве описания исходных данных // Вестник Восточно-Сибирского института МВД России: науч.-практич. журн. Иркутск: Восточно-Сибирский институт МВД России. 2024. № 1(108). С. 166–177. DOI: 10.55001/2312-3184.2024.88.52.014

9. Душкин А. С., Федотова Е. С. Оценка риска совершения преступлений лицами, освобожденными из мест лишения свободы. Российский девиантологический журнал. 2024. № 4 (1). С. 45-61. doi: 10.35750/2713-0622-2024-1-45-61.

10. Жмуров Д. В. Прогнозирование преступности в контексте глобальных проблем человечества // Академический юридический журнал. 2025. Т. 26, № 1. С. 133–141. DOI 10.17150/1819-0928.2025.26(1).133-141. EDN IRPPZD

11. Кудрявцев В. Н. Генезис преступления. Опыт криминологического моделирования: учебное пособие. М.: Инфра-М, 1998. 216 с.

12. Майоров А. В. Частная методика прогнозирования и моделирования виктимологической ситуации // Юридическая наука и правоохранительная практика. 2020. № 4 (54). С. 52-58.

13. Терехов А. М., Кувычков С. И., Смирнов С. А. Особенности статистического моделирования и прогнозирования преступности: теоретический аспект // Юридическая наука и практика: Вестник нижегородской академии МВД России. 2021. № 2. С. 123-130.

14. Berk Richard Forecasting Methods in Crimeand Justice The Annual Review of Lawand Social Science, 2008, 4. P. 219-238.

15. Dumanskaya E.I., Emelyanov I.G. Mathematical Monitoring of the Human Criminal Behavior System. Procedia Structural Integrity. 2024. 65. P. 75–82. DOI 10.1016/j.prostr.2024.11.012.

16. Emel'yanov I. G., Dumanskaya E. I. Crime-related Threats on Transportation Safety: A Mathematical Model of Risk Assessment. In Proceedings of the 1st International Scientific and Practical Conference on Transport: Logistics, Construction, Maintenance, Management – TLC2M-2022; ISBN 978-989-758-606-4, SciTePress, pages 272-277. TLC2M_2022.pdf (40512909). DOI: 10.5220/0000165000003527.

17. Farrington D. P., MacLeod J.F. and Piquero A. R., Mathematical Models of Criminal Careers: Deriving and Testing Quantitative Predictions, Journal of Research in Crime and Delinquency. 2016, Vol. 53(3). P. 336-355

18. Feroz Shah Syed, Didong Li, Xun Zhang and Zhenhong Guo, Mathematical Modelling in Criminology Malaysian Journal of Mathematical Sciences. 2013, 7(1): 125-145

19. Hamilton M. Judicial gatekeeping on scientific validity with risk assessment tools. Behav Sci Law. 2020; 38:226–245. https://doi.org/10.1002/bsl.2456

20. Hester R. Risk assessment savvy: The imperative of appreciating accuracy and outcome. Behav Sci Law. 2020; 1–13. doi.org/10.1002/bsl.2457

21. Prins Seth, Reich Adam, Criminogenic risk assessment: A meta-review and critical analysis Punishm Soc. 2021 Jun 30; 23(4):578–604. doi: 10.1177/14624745211025751

22. Simon Jonathan REVERSAL OF FORTUNE: The Resurgence of Individual Risk Assessment in Criminal Justice Annu. Rev. Law Soc. Sci. 2005. 1:397–421 doi: 10.1146/annurev.lawsocsci.1.041604.120006

23. Skeem J., Lowenkamp C. Risk, race, and recidivism: predictive bias and disparate impact. Criminology, 2016, Volume 54 Number 4, 680–712, doi: 10.1111/1745-9125.12123

24. Srivastav A.K., Athithan S. Modeling and analysis of crime prediction and prevention, Social Network Analysis and Mining, 2020, 10:26. DOI 10.1007/s13278-020-00637-8.

УДК 343.632

Л. Ю. Зеленова,
преподаватель высшей категории,
Челябинский государственный университет

Особенности кибербуллинга несовершеннолетних и важность его специального изучения (правовой аспект)

Аннотация. Статья посвящена актуальной проблеме цифровой эпохи – кибербуллингу несовершеннолетних. Автор проводит сравнительный анализ кибербуллинга и традиционного школьного буллинга, выделяя ключевые отличия, которые обуславливают повышенную опасность первого: анонимность агрессора, перманентность и вирусный характер распространения контента, отсутствие безопасного пространства для жертвы. Цель статьи – на основе сравнительно-правового анализа подчеркнуть, что существующие правовые нормы (о клевете, оскорблении и др.) недостаточно эффективны для противодействия систематическому кибербуллингу, и обосновать необходимость разработки специальных правовых механизмов. В статье рассматриваются возможные пути совершенствования законодательства, включая введение административного запрета на кибербуллинг. Делается вывод о том, что решение проблемы требует комплексного подхода, сочетающего правовые, педагогические и воспитательные меры.

Ключевые слова: кибербуллинг, традиционный буллинг, интернет-травля, несовершеннолетние, правовая защита, цифровая среда, сравнительный анализ, профилактика

L. Y. Zelenova,
Teacher of the highest category,
Chelyabinsk State University

Features of juvenile cyberbullying and the importance of its special study (legal aspect)

Abstract. The article is devoted to an urgent problem of the digital age – cyberbullying of minors. The author conducts a comparative analysis of cyberbullying and traditional school bullying, highlighting the key differences that cause the increased danger of the former: the anonymity of the aggressor, the permanence and viral nature of content distribution, and the lack of a safe space for the victim. The purpose of the article is to emphasize, based on a comparative legal analysis, that the existing legal norms (on libel, insult, etc.) are not effective enough to counteract systematic cyberbullying, and to justify the need to develop special legal mechanisms. The article discusses possible ways to improve legislation, including the introduction of an administrative ban on cyberbullying. It is concluded that solving the problem

requires an integrated approach combining legal, pedagogical and educational measures.

Keywords: cyberbullying, traditional bullying, online harassment, minors, legal protection, digital environment, comparative analysis, prevention

Введение. Многие преподаватели, работающие со школьниками и студентами, ежедневно сталкиваются с тем, что жизнь современных подростков неразрывно связана с цифровой средой. Это пространство не только возможностей, но и новых, цифровых рисков. Сегодня, одним из самых серьезных вызовов уже стал кибербуллинг, который, по сути, является эволюцией старой, как мир, школьной травли. Но если с обычным буллингом хотя бы примерно понятно, как бороться, то его цифровой «собрат» ставит в тупик и педагогов, и правоохранителей.

Цель этой статьи не просто описать явление, а показать, чем кибербуллинг фундаментально отличается от традиционной травли и почему эти отличия требуют особого, в том числе правового, подхода. К сожалению, представляется, что нельзя бороться с новой угрозой старыми методами.

Основная часть. Чтобы понять уникальность кибербуллинга, проведем прямое сравнение с его «аналоговым» предшественником (табл. 1).

Таблица 1

Сравнительный анализ традиционного буллинга и кибербуллинга

Критерий	Традиционный буллинг	Кибербуллинг
Анонимность	Агрессор известен, часто это физически сильный лидер или группа. Конфликт лицом к лицу	Ключевая особенность. Агрессор может скрываться за фейковым аккаунтом, что развязывает ему руки и усугубляет жестокость [1]
Аудитория	Ограничена учебным заведением, двором, районом. Свидетелей чаще всего немного, а те, которые есть, либо поддерживают агрессора, либо отстраняются от ситуации	Потенциально бесконечная. Унизительный контент за минуты может стать достоянием не только всего образовательного учреждения, но и города, страны [2]
Время и место	Имеет временные и пространственные границы: за пределами учебного заведения травля чаше прекращается	Не имеет границ. Травля продолжается 24/7, проникая через смартфоны, планшеты и компьютеры в личную комнату жертвы, лишая ее последнего убежища [3]
Физическая сила	Часто основан на физическом или материальном превосходстве агрессора	Не важна. Жертвой может стать и физически сильный подросток. Важнее цифровая грамотность и доступ к личной информации

Критерий	Традиционный буллинг	Кибербуллинг
След	Эфемерен: обидные слова забываются, синяки проходят. Агрессор взрослеет и теряет интерес к жертве	Перманентность цифрового контента. Скриншоты, перепосты, сохраненные видео практически невозможно удалить из сети полностью. Это «пятно», которое может преследовать человека годами [4]

Это сравнение наглядно показывает, что кибербуллинг – это не просто «травля в интернете». Это качественно новое, более опасное явление, обладающее собственной природой и динамикой.

Здесь мы подходим к главной проблеме. Российское законодательство пока пытается бороться с цифровым моном аналоговым оружием.

Действующие нормы (ст. 128.1 УК РФ «Клевета», ст. 5.61 КоАП РФ «Оскорбление», ст. 137 УК РФ «Нарушение неприкосновенности частной жизни», и даже ст. 110 «Доведение до самоубийства») направлены на борьбу с единичными, изолированными правонарушениями. Они плохо ловят систематичность – основную черту буллинга. Один оскорбительный комментарий – это административное правонарушение. Но десятки таких комментариев ежедневно, создание унижающих мемов, организация бойкота в чате – это уже не набор отдельных правонарушений, а целенаправленная кампания по уничтожению личности. Именно эту системность законодатель и не улавливает.

Кроме того, процессуальные барьеры, например, необходимость установления личности анонимного агрессора, которая требует сложных и долгих процедур взаимодействия с провайдерами, часто делают обращение в правоохранительные органы бессмысленным для подростка, который ждет помощи здесь и сейчас.

Исходя из вышеизложенного, видится, что работа должна вестись на двух фронтах: правовом и педагогическом.

1. Необходимо введение в КоАП РФ отдельной статьи «Кибербуллинг», которая бы учитывала его системную природу. Это позволило бы привлекать хотя бы административной ответственности не только самих несовершеннолетних агрессоров (с 16 лет), но и возлагать административную ответственность на родителей, мотивируя их к контролю за онлайн-активностью детей.

2. В педагогическом направлении ключом может стать профилактика. Необходимо в образовательные программы колледжей и школ включить модули по цифровой грамотности и кибербезопасности, где на реальных кейсах объяснять не только юридические, но и моральные последствия травли. Проводить индивидуальные и групповые встречи с психологами для выявления зреющих конфликтов и их пресечения на ранних стадиях. Работа с родителями в части их обучения тактике поведения при выявлении ситуаций с кибербуллинга в отношении или от имени их ребенка.

Итак, очевидно, что кибербуллинг – это не просто «Буллинг 2.0», а принципиально иное, цифровое явление, трансформационные отличия которого (анонимность, масштаб, перманентность и отсутствие границ), создают качественно новую угрозу для здоровья подростков и, в целом, здоровья общества.

Заключение. Существующая правовая система, к сожалению, отстает от реалий цифрового мира. Она борется с симптомами (отдельными оскорблениями или клеветой), но не с болезнью – систематической цифровой травлей. Педагогам и юристам, необходимо выступать за принятие специальных правовых норм, которые бы адекватно реагировали на вызовы времени. Без этого все разговоры о безопасности детей в интернете останутся просто благими пожеланиями. Защита молодого поколения требует новых, современных решений.

Список литературы

1. Hinduja, S., & Patchin, J. W. (2021). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying (3rd ed.). Corwin.

2. Фонд «Общественное мнение» (ФОМ). (2022). Подростки в интернете: риски и безопасность. [Электронный ресурс]. URL: https://fom.ru/

3. Солдатова, Г.У., Шляпников, В.Н. (2020). Цифровая компетентность подростков и родителей: результаты всероссийского исследования. М.: Фонд Развития Интернет.

4. Kowalski, R. M., Limber, S. P., & McCord, A. (2019). A developmental approach to cyberbullying: Prevalence and protective factors.

5. Казаков, Б.А. (2021). Уголовно-правовая характеристика кибербуллинга: проблемы квалификации. Вестник университета им. О.Е. Кутафина (МГЮА), (5), 192-199.

УДК 343.85

А. А. Зеленцов,
кандидат юридических наук, доцент,
Санкт-Петербургский университет МВД России

Криминологические и виктимологические особенности киберпреступности в современной России

Аннотация. В статье анализируются современные тенденции киберпреступности в России через призму криминологических и виктимологических подходов. Рассматриваются основные виды киберпреступлений, их количественные и качественные показатели, факторы виктимизации населения, а также меры противодействия. Использованы данные МВД, ФСБ и экспертных отчетов за 2024–2025 годы. Особое внимание уделяется роли искусственного интеллекта, социальной инженерии и международного сотрудничества в борьбе с цифровой преступностью.

Ключевые слова: киберпреступность, виктимология, криминология, цифровая безопасность, Россия, кибермошенничество, профилактика

A. A. Zelentsov,
Candidate of Legal Sciences, Associate Professor,
St. Petersburg University of the Ministry of Internal Affairs of Russia

Criminological and victimological features of cybercrime in modern Russia

Abstract. The article analyzes modern trends in cybercrime in Russia through the prism of criminological and victimological approaches. The main types of cybercrimes, their quantitative and qualitative indicators, factors of population victimization, as well as countermeasures are considered. Data from the Ministry of Internal Affairs, the FSB, and expert reports for 2024–2025 are used. Special attention is paid to the role of artificial intelligence, social engineering, and international cooperation in the fight against digital crime.

Keywords: cybercrime, victimology, criminology, digital security, Russia, cyber fraud, prevention

Введение. Киберпреступность стала одним из наиболее динамично развивающихся видов преступности в современной России. В 2024 году доля преступлений, совершенных с использованием информационных технологий, составила 40% от общего числа правонарушений, а ущерб превысил 170 млрд рублей [1]. Это обусловлено цифровизацией всех сфер жизни, расширением использования облачных сервисов и активным внедрением технологий искусственного интеллекта (далее – ИИ) преступными группами. В таких условиях необходимо комплексное изучение киберпреступности не только с криминоло-

гических, но и с виктимологических позиций, чтобы понять механизмы виктимизации и разработать эффективные профилактические меры.

Основная часть.

1. Криминологическая характеристика киберпреступности в России.

В 2024 году киберпреступность в России продемонстрировала качественно новые характеристики. По данным ГИАЦ МВД России, общее число зарегистрированных преступлений в цифровой среде достигло 765,4 тыс., что составляет 40,2% от общего массива преступности в стране. По сравнению с 2023 годом прирост составил 13,1%, при этом необходимо отметить, что латентность данного вида преступлений оценивается экспертами на уровне 60-70%.

Доля видов преступлений в сфере информационных технологий в общем количестве зарегистрированных киберпреступлений (2024 г.):

– мошенничества, совершаемые с использованием информационно-телекоммуникационных технологий (ст. 159 УК РФ) – 49,7% (380,3 тыс.);

– преступления, связанные с неправомерным оборотом платежных карт – 15,1% (115,5 тыс.);

– неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ) – 13,8% (105,8 тыс.);

– создание, использование и распространение вредоносных компьютерных программ – 8,4%(64,3 тыс.);

– преступления против общественной безопасности, связанные с использованием IT (кибертерроризм) – 3,5%(26,8 тыс.);

– иные преступления в сфере информационных технологий – 9,5%·(72,7 тыс.).

Анализ территориального распределения показывает значительную неравномерность. Наибольшая концентрация киберпреступлений отмечается в регионах с высоким уровнем цифровизации и развитой IT-инфраструктурой:

Регионы-лидеры по удельному весу киберпреступлений (2024 г.):

Республика Мордовия – 63,4%;

Республика Марий Эл – 61,6%;

Республика Татарстан – 57,1%;

Москва – 52,8%;

Санкт-Петербург – 49,3%.

Наименьшие показатели наблюдаются в регионах с низким уровнем интернет-проникновения:

Чеченская Республика – 16,6%;

Республика Дагестан – 15,1%;

Республика Тыва – 17,2% [5].

Рассматривая технологическую эволюцию киберпреступности в 2024-2025 годах, специалисты отмечают массовое внедрение AI-технологий в киберпреступную деятельность (генеративные состязательные сети (GAN) для создания дипфейков, нейросети Transformer для фишинговых атак, автоэнкодеры для обхода систем обнаружения вторжений), развитие квантовых вычислений создает новые риски (угроза взлома асимметричных криптосистем (RSA, ECC), необхо-

димость перехода на постквантовые алгоритмы шифрования, риски для блокчейн-систем и цифровой идентификации). Статистика 2024 года показывает:

– 22% атак на крупные компании осуществлены через уязвимости в стороннем ПО;

– среднее время обнаружения compromise – 287 дней;

– ущерб от одной успешной атаки – в среднем 4,45 млн долларов [2].

Современная киберпреступность давно перестала быть уделом одиночек-хакеров, работающих в подполье ради славы. Сегодня это высокоорганизованная, глобальная и чрезвычайно прибыльная индустрия, по своей структуре и подходу все чаще напоминающая легальный бизнес.

Киберпреступные сообщества превратились в полноценные корпорации теневого цифрового мира. Их главная характеристика – высочайший уровень профессионализации.

Вместо разрозненных групп здесь действуют строго структурированные организации с четким разделением труда [4]. Как в обычной IT-компании, здесь есть свои разработчики, которые создают вредоносное ПО и эксплойты [7]; аналитики, исследующие уязвимости и выбирающие цели; и операторы, которые непосредственно проводят атаки и взаимодействуют с жертвами. Это позволяет нанимать узкоспециализированных экспертов и масштабировать операции.

Криминальные группы активно перенимают и современные бизнес-модели, такие как RaaS (Ransomware-as-a-Service – «вымогательство как услуга») и MaaS (Malware-as-a-Service – «вредоносное ПО как услуга»). По этой модели создатели вирусов-вымогателей или другого опасного ПО не атакуют сами, а сдают свое «ноу-хау» в аренду менее квалифицированным преступникам за долю с прибыли. Это резко снижает порог входа в криминальный бизнес и приводит к взрывному росту числа атак.

Результатом такой организации становится колоссальный денежный поток. Среднемесячный доход организованных киберпреступных групп оценивается как минимум в 200 млн рублей, что сравнимо с прибылью среднего легального предприятия.

Киберпреступность не знает национальных границ, что делает ее одной из самых глобальных угроз современности.

78% всех кибератак имеют международную составляющую. Это означает, что злоумышленники, инфраструктура для атаки, жертвы и процедура отмывания денег могут находиться в совершенно разных уголках планеты, что крайне затрудняет расследование и противодействие.

Согласно статистике, основными странами-источниками киберугроз являются:

Китай (32%) – часто ассоциируется с целевыми атаками на бизнес и государственные структуры с целью промышленного шпионажа.

Нигерия (24%) – традиционный центр мошеннических схем, таких как «нигерийские письма» (BEC-мошенничество) и романтический скам.

Украина (18%) – известна высококвалифицированными IT-специалистами, которые часто вовлечены в создание сложного вредоносного ПО и операции с RaaS [4].

Для обналичивания и легализации своих доходов преступники массово используют криптовалюты. Анонимность и децентрализация блокчейна позволяют эффективно скрывать движение средств. Более 45% всех незаконных финансовых операций в киберпространстве проводятся с использованием криптовалют, что представляет серьезный вызов для правоохранительных органов по всему миру.

Таким образом, киберпреступность эволюционировала в слаженную транснациональную индустрию с отлаженными бизнес-процессами, что требует адекватного и столь же система подхода к кибербезопасности на государственном и международном уровне.

Киберпреступность нанесла российской экономике в 2024 году колоссальный и многомиллиардный ущерб, который по оценкам Центробанка РФ распределился по всем секторам. Суммарные потери оказались огромными: 84,3 млрд. рублей составил ущерб для физических лиц, 67,2 млрд. рублей – для бизнеса и 18,9 млрд. рублей – для государственных учреждений. Таким образом, общая сумма финансовых потерь превысила 170 млрд рублей [1].

Наиболее тяжелый удар пришелся на ключевые отрасли экономики. Абсолютным лидером по объему потерь стал финансовый сектор, на который пришлось 43% общего ущерба. Немногим менее четверти всех убытков (22%) сконцентрировалось в сфере телекоммуникаций. Критически важная энергетическая инфраструктура понесла ущерб в 15% от общей суммы, а система здравоохранения – 12%. Эта статистика наглядно демонстрирует, что злоумышленники целенаправленно атакуют наиболее чувствительные и значимые для общества и экономики области.

Несмотря на масштаб угроз, эффективность противодействия киберпреступности со стороны правоохранительной системы, по текущим данным, остается недостаточной. Это проявляется в ключевых показателях раскрываемости и доведения дел до логического завершения.

Так, уровень раскрываемости киберпреступлений остается низким и составляет лишь 28,4%. Это означает, что более семи из десяти инцидентов не находят своего виновника. Даже в случае возбуждения уголовного дела до суда доходит лишь 63,2% из них, что свидетельствует о сложностях в сборе неопровержимых цифровых доказательств. Для тех преступников, которых все же осуждают по статье 272 УК РФ (неправомерный доступ к компьютерной информации), средний срок лишения свободы составляет 3,8 года [5].

Совокупность этих данных убедительно свидетельствует о наличии системных проблем и острой необходимости дальнейшего совершенствования как технических возможностей по отслеживанию и профилактике кибератак, так и правовых механизмов, включая адаптацию законодательства и повышение квалификации следственных органов.

Виктимология киберпреступности – это область знаний, изучающая жертв цифровых преступлений: их характеристики, поведение, которое привело

к виктимизации (становлению жертвой), и многообразные последствия этого опыта. В отличие от традиционной преступности, где жертва и преступник зачастую находятся в физическом контакте, в киберпространстве жертва обычно анонимна и обезличена для атакующего, который действует на расстоянии, что создает уникальные психологические и практические трудности.

Жертвой киберпреступления может стать абсолютно любой человек, пользующийся цифровыми технологиями. Однако статистика и практика выявляют группы повышенного риска, а также модели поведения, которые значительно увеличивают уязвимость [3].

Наиболее уязвимыми группами являются люди, оказавшиеся на своеобразных «окраинах» цифрового мира. Во-первых, это лица с низкой цифровой грамотностью, часто старшего возраста. Они могут не распознать признаки поддельного письма, маскирующегося под официальное сообщение от банка или государственной службы. Их доверчивость и незнание базовых правил кибергигиены делают их легкой добычей для социальной инженерии.

Во-вторых, в группе риска находятся активные пользователи социальных сетей и мобильных устройств, особенно подростки и молодые взрослые. Хотя они технически подкованы, их психологическая уязвимость является результатом потребности в социальном одобрении, любопытства и склонности к рискованному поведению онлайн. Они чаще переходят по сомнительным ссылкам, участвуют в вирусных испытаниях, требующих предоставления личных данных, и чрезмерно делятся подробностями своей жизни, создавая идеальную основу для шантажа, кражи личных данных или кибербуллинга.

Ключевой аспект, объединяющий жертв, – это не столько возраст или профессия, сколько поведенческие паттерны. Наиболее разрушительными являются:

Пренебрежение к паролям: Использование простых, предсказуемых паролей (типа «123456», «qwerty») или одного пароля для множества сервисов. Отсутствие многофакторной аутентификации, которая является мощнейшим барьером, лишает пользователя последней линии обороны [3].

Неосторожное обращение с персональными данными: Публикация в открытых источниках информации о месте жительства, графике работы, дорогих покупках, отпусках, а также ответы на якобы безобидные «опросники» в соцсетях (девичья фамилия матери, кличка первого питомца) предоставляет злоумышленникам полный комплект данных для взлома аккаунтов или социальной инженерии.

Последствия кибератаки далеко не всегда ограничиваются материальным ущербом, зачастую психологическая травма оказывается глубокой и продолжительной.

Причины становления жертвой лежат в двух плоскостях: человеческой ошибке и технологическом несовершенстве [3].

Человеческий фактор: это самый слабый элемент любой системы защиты. До 44% утечек данных в российских компаниях происходят из-за непреднамеренных действий сотрудников. Это может быть письмо с вложенным вредоносным файлом, отправленное на личную почту, использование незащищенных

публичных Wi-Fi сетей для работы с корпоративными данными, или банальная потеря служебного устройства. Преступники мастерски манипулируют людьми, играя на их любопытстве, страхе или желании помочь, обходя таким образом даже самые продвинутые технические средства защиты.

Технические факторы: со стороны организаций уязвимость создает халатность или некомпетентность в настройке IT-инфраструктуры. Неправильная конфигурация облачных сервисов, оставляющая базы данных открытыми для всех в интернете, использование устаревшего программного обеспечения с известными, но не исправленными уязвимостями (например, Windows 7), отсутствие систем постоянного мониторинга и обнаружения аномальной активности – все это открытые двери для злоумышленников. Часто компании экономят на кибербезопасность, ошибочно полагая, что с ними ничего не случится, что и делает их легкой мишенью.

Таким образом, портрет жертвы киберпреступления складывается из комбинации личностных, поведенческих и организационных факторов. Борьба с киберпреступностью требует не только совершенствования технологий, но и массового повышения цифровой грамотности, формирования культуры кибербезопасности на уровне каждого отдельного пользователя и целой организации.

Эффективная защита от современных киберугроз требует комплексного подхода, объединяющего правовые, технологические, организационные и человеческие аспекты. Меры должны быть выстроены в единую экосистему безопасности, где каждый элемент усиливает другой.

1. Государственные и правовые механизмы: Формирование надежного правового поля. Данный уровень является фундаментальным и направлен на создание единой общегосударственной стратегии, установление четких правил и разработку эффективных механизмов противодействия киберугрозам. Его реализация состоит из трех последовательных шагов [3].

Шаг 1: Совершенствование национального законодательства и нормативной базы.

Без прочной, устойчивой, всеобъемлющей и эффективной системы законов и нормативных актов все остальные меры (технические, организационные, международные) будут неполноценными или неработающими. Ключевые действия на этом этапе:

– сертификация и стандартизация: Первоочередная задача – разработка и внедрение обязательных национальных стандартов кибербезопасности для критической информационной инфраструктуры, органов государственной власти и всех операторов персональных данных. Это создаст базовый уровень защищенности;

– ужесточение ответственности: Следующий шаг – введение суровых санкций за несоблюдение установленных стандартов. Повышенные административные штрафы (например, до 15 млн рублей для бизнеса) и, что ключевое, уголовная ответственность за сокрытие фактов утечек, а также за приобретение и использование украденных данных создают прямые финансовые и репутационные риски, заставляя организации соблюдать требования;

– стимулирующее регулирование: для дальнейшего снижения рисков необходимо внедрить механизмы киберстрахования (как обязательного или поощряемого условия). Это перераспределит финансовую нагрузку и создаст для рынка дополнительный стимул к повышению собственной безопасности, так как страховые компании будут оценивать риски.

Шаг 2: Развитие национального потенциала и кадрового обеспечения.

Укрепленная нормативная база требует внутренних ресурсов для своей реализации.

Подготовка кадров: для выполнения новых требований необходимы квалифицированные специалисты. Следует ввести специализированные образовательные программы в вузах и колледжах по подготовке экспертов в сфере кибербезопасности, реализуемые в партнерстве с ведущими IT-компаниями.

Поддержка отечественных решений: параллельно необходимо стимулировать импортозамещение в сфере информационной безопасности через госзаказы, гранты и налоговые льготы для отечественных компаний-разработчиков. Это создаст технологический суверенитет и укрепит экономику.

Шаг 3: Активное международное сотрудничество и дипломатия.

Киберугрозы не признают национальных границ, поэтому локальных мер недостаточно. Завершающий этап – выход на международный уровень.

Обмен информацией: Базовый уровень кооперации – налаживание доверительных каналов оперативного обмена данными об угрозах между национальными командами по реагированию на компьютерные инциденты разных стран.

Создание альянсов: более глубокая форма сотрудничества – формирование международных коалиций для совместного отслеживания и пресечения деятельности транснациональных хакерских группировок по аналогии с борьбой с пиратством.

Разработка единых норм: Стратегическая цель – активная работа по созданию международной конвенции по кибербезопасности под эгидой ООН. Ее задачи: определение неприемлемого поведения в киберпространстве, установление правил ведения кибервойн и создание работающих механизмов экстрадиции киберпреступников.

2. Технологические решения для построения эшелонированной обороны.

Современный ландшафт угроз требует перехода от единой линии обороны (периметра) к многоуровневой, адаптивной и проактивной модели безопасности. Защита должна выстраиваться эшелонами, где каждый уровень обеспечивает свою функцию, а их совместная работа создает комплексный барьер для злоумышленника.

Последовательность построения такой обороны можно разделить на три ключевых этапа [2]:

1 этап. Фундамент: Новая парадигма доступа и контроля (Zero Trust – нулевое доверие).

Основой современной защиты должен стать принцип – «Никому не доверяй, проверяй всегда». Это означает отказ от модели, где все внутри сети считается безопасным, и переход к постоянной проверке каждого запроса на доступ.

Строгая идентификация и аутентификация: Каждый пользователь и устройство должны быть однозначно идентифицированы и верифицированы с помощью многофакторной аутентификации перед получением доступа.

Принцип наименьших привилегий: Пользователям и приложениям предоставляется доступ только к тем ресурсам, которые абсолютно необходимы для выполнения их задач, и только на ограниченное время.

Микросетевание: Внутренняя сеть делится на небольшие изолированные сегменты (зоны). Это предотвращает горизонтальное перемещение злоумышленника и локализует потенциальный инцидент в случае взлома.

2 этап. Оперативный эшелон: Проактивное обнаружение и прогнозирование угроз. После внедрения базовых контролей доступа необходимо усилить оборону системами, способными выявлять сложные и ранее неизвестные атаки.

Искусственный интеллект и машинное обучение (AI/ML):

Анализ поведения (UEBA): Системы анализируют шаблоны поведения пользователей и систем, чтобы выявлять аномалии и подозрительную активность, что критически важно для обнаружения атак типа Zero-day.

Автоматизация SOC (SOAR): Платформы автоматизируют сбор данных с различных источников, корреляцию событий и процедуры реагирования, что значительно ускоряет время реакции на инциденты.

Борьба с компрометирующим контентом: Разработка и внедрение инструментов на основе искусственного интеллекта для автоматического обнаружения дипфейков и синтезированных медиафайлов.

Подготовка к будущим угрозам:

Постквантовая криптография: уже сегодня необходимо начинать разработку, тестирование и постепенное внедрение алгоритмов шифрования, устойчивых к взлому с помощью квантовых компьютеров, чтобы защитить критичные данные в долгосрочной перспективе.

3 этап. Завершающий эшелон: Обеспечение устойчивости и целостности.

Ни одна система не является неприступной. Финальный рубеж обороны предназначен для минимизации ущерба и быстрого восстановления работоспособности в случае успешной атаки.

Стратегия резервного копирования и восстановления:

– Внедрение отказоустойчивых и географически распределенных систем резервного копирования.

– Регулярное и обязательное тестирование процедур аварийного восстановления. Это главный инструмент противодействия атакам программ-вымогателей, позволяющий восстановить данные без выплаты выкупа.

Защита цепочек поставок:

– Тщательная проверка безопасности стороннего программного обеспечения и оборудования перед их внедрением в инфраструктуру.

– Использование реестров программных компонентов (SBOM) для обеспечения прозрачности и контроля за используемыми библиотеками и их уязвимостями.

Таким образом, эшелонированная оборона строится последовательно: от фундамента в виде контроля доступа по модели «нулевое доверие», через внед-

рение интеллектуальных систем обнаружения к созданию надежных планов обеспечения устойчивости бизнеса.

3. Образовательные и организационные меры: Человек как ключевое звено защиты. Самые совершенные технологии бесполезны, если ими не умеют правильно пользоваться и если не выстроены необходимые процедуры [3].

– Постоянное обучение и повышение грамотности.

Программы для конкретных целей: Проведение не для галочки, а практических тренингов для разных групп пользователей: обычных сотрудников, высшего руководства, специалистов по информационным технологиям.

Обучающие форматы с погружением: Применение игровых методов, учебных имитаций взломов и виртуальных учений для отработки навыков в условиях, близких к реальности. Это помогает выработать автоматические реакции и правильные модели поведения.

Просвещение широких слоев населения: Государственные и общественные программы по повышению компьютерной грамотности граждан, особенно для наиболее уязвимых групп (пенсионеры, дети).

– Формирование культуры безопасной работы.

Внедрение внутренних правил: Разработка четких и понятных инструкций, которые регулируют работу с данными, использование личных устройств на работе, правила создания паролей и поведение в социальных сетях.

Ответственность руководства: Безопасность – это не только задача технических специалистов, но важнейшая обязанность высших руководителей (например, директора по безопасности, генерального директора). Необходимо включать вопросы цифровых угроз в общую систему управления рисками компании.

Создание положительной мотивации: Поощрение сотрудников, которые сообщают о подозрительных письмах или происшествиях, а не их наказание. Это способствует созданию обстановки открытости и доверия.

– Налаживание процедур реагирования на происшествия.

Разработка планов реагирования: Наличие заранее подготовленных схем действий при различных типах нарушений (утечка данных, вымогательство, атаки на отказ в обслуживании).

Регулярные проверки и испытания: Проведение тестов на защищенность и проверок для независимой оценки уровня безопасности и своевременного выявления слабых мест.

Только синтез строгого законодательства, передовых технологий и высокой осведомленности человека позволяет создать устойчивую и проактивную систему противодействия киберугрозам, способную адаптироваться к постоянно меняющемуся ландшафту рисков.

Проведенное исследование криминологических и виктимологических аспектов киберпреступности в современной России позволяет сформулировать следующие выводы и рекомендации:

1. Качественная трансформация киберпреступности: В 2024-2025 годах произошла фундаментальная эволюция от единичных компьютерных инцидентов к сложным системным атакам, использующим искусственный интеллект и

квантовые технологии. Доля киберпреступлений в общем массиве преступности достигла 40,2%, что свидетельствует о переходе к новой парадигме цифровой преступности [6].

2. Технологическая изощренность: отмечается переход от традиционных вредоносных программ:

– к AI-генеративным атакам (дипфейки, адаптивные фишинговые системы);

– квантово-криптографическим методам взлома;

– атакам на цепочки поставок с периодом скрытого присутствия до 287 дней.

3. Организационная структура: Современные киберпреступные сообщества функционируют по модели транснациональных корпораций со строгой специализацией и годовым оборотом, превышающим 2,4 млрд. рублей. 78% атак имеют международный характер [4].

4. Виктимологический аспект: Выявлена четкая корреляция между уровнем цифровой грамотности и риском виктимизации. Наиболее уязвимые группы:

– лица старше 55 лет (62% жертв финансового мошенничества);

– активные пользователи социальных сетей (87% случаев кражи персональных данных);

– сотрудники компаний с недостаточной киберкультурой (44% успешных атак) [3].

5. Экономические последствия: Совокупный ущерб превысил 170 млрд. рублей, при этом лишь 28,4% преступлений раскрывается. Наиболее уязвимые сектора:

– Финансовый (43% ущерба);

– Критическая информационная инфраструктура (37%);

– Государственный сектор (12%) [6].

Перспективные направления противодействия:

1. Технологическая модернизация:

– Внедрение постквантовых алгоритмов шифрования до 2026 года [2];

– Развертывание национальной системы AI-детекции кибератак;

– Создание единой платформы мониторинга критической инфраструктуры.

2. Правовое регулирование:

– Разработка федерального закона «О кибербезопасности критической информационной инфраструктуры» [3].

– Введение уголовной ответственности за создание и использование дипфейков в преступных целях.

– Усиление мер ответственности за неправомерное использование персональных данных.

3. Организационные меры:

– Создание национального центра реагирования на киберинциденты.

– Разработка единых стандартов кибергигиены для различных категорий пользователей.

– Внедрение обязательного страхования киберрисков для компаний КИИ [3].

4. Международное сотрудничество:

– Формирование единого правового поля в рамках ЕАЭС.

– Участие в разработке международной конвенции по киберпреступности.

– Создание трансграничных механизмов отслеживания криптовалютных операций.

5. Научно-исследовательская деятельность:

– Разработка прогнозных моделей развития киберпреступности до 2030 года.

– Проведение междисциплинарных исследований в области цифровой виктимологии.

– Создание центра компетенций по квантовой безопасности [2].

Заключение. Киберпреступность в России превратилась в системную угрозу национальной безопасности, требующую комплексного межведомственного подхода [8, 9]. Необходима консолидация усилий государства, бизнеса и гражданского общества для формирования устойчивой цифровой среды. Приоритетом должна стать опережающая разработка защитных механизмов против угроз следующего поколения, основанных на квантовых вычислениях и искусственном интеллекте. Цифровая сфера является «серой зоной» с неопределенными правовыми принципами, что осложняет вопрос о том, являются ли кибератаки на самом деле преступными или нет [8. С. 994].

Дальнейшие исследования должны быть сфокусированы на разработке предиктивных моделей кибервиктимизации и создании адаптивных систем защиты, способных противодействовать угрозам 2030-х годов.

Список литературы

1. В России в 2024 году IT-преступления достигли пика за последние пять лет // URL: https://tass.ru/proisshestviya/22978955 (дата обращения: 25.08.2025).

2. Квантовые вычисления и кибербезопасность: разбираемся в технологиях будущего // URL: https://habr.com/ru/companies/ddosguard/articles/901766/ (дата обращения: 25.08.2025).

3. Кибербезопасность 2025. Анализ и рекомендации. URL: https://globalcio.ru/discussion/47735/ (дата обращения: 25.08.2025).

4. Проект 2030: киберугрозы для подключенного мира. URL: https://habr.com/ru/companies/trendmicro/articles/595719/ (дата обращения: 25.08.2025).

5. Статистика киберпреступности в российских регионах: данные МВД за 2024 год // URL: https://www.ec-rs.ru/blog/novosti/statistika-kiberprestupnosti-v-rossiyskikh-regionakh-dannye-mvd-za-2024-god/ (дата обращения: 25.08.2025).

6. Число IT-преступлений в 2024 году достигло рекордных значений. URL: https://expert.ru/news/chislo-it-prestupleniy-v-2024-godu-dostiglo-v-rossii-rekordnykh-765-4-tys/(дата обращения: 25.08.2025).

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

8. Аувал А.М., Лазарус С. Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности // Journal of Digital Technologies and Law. 2024. Т. 2, № 4. С. 915-942. https://doi.org/10.21202/jdtl.2024.44. EDN: JVGLRH.

9. Рахман М.М., Дас Т.К. Противодействие кибератакам: пробелы международного права и перспективы их преодоления // Journal of Digital Technologies and Law. 2024. Т. 2, № 4. С. 973 1002. https://doi.org/10.21202/jdtl.2024.46. EDN: NNFTQI.

УДК 343.7+343.988

А. В. Майоров,
доктор юридических наук, доцент,
Уральский государственный юридический университет
имени В. Ф. Яковлева

Уголовно-правовое предупреждение цифровой виктимности несовершеннолетних

Исследование выполнено за счет гранта Российского научного фонда
№ 25-18-00881

Аннотация. Статья посвящена анализу современных тенденций в области цифровизации и ее влияния на взаимодействие и жизнедеятельность людей, с особым акцентом на проблемы, связанные с использованием интернет-ресурсов несовершеннолетними. Автор рассматривает масштабное внедрение цифровых технологий, опирающихся на искусственный интеллект и программные продукты, которые активно трансформируют традиционные формы общения и жизнедеятельности, особенно в контексте социальных сетей и мессенджеров, наиболее популярных среди подростков и молодежи. Центральной темой исследования является вопрос о низком уровне цифровой и информационной защиты несовершеннолетних пользователей, что напрямую связано с ростом цифровой виктимности среди этой категории населения, а также необходимой уголовно-правовой охраной. Рассматривается уголовно-правовой механизм снижений цифровой виктимности несовершеннолетних.

Ключевые слова: виктимизация, виктимизация несовершеннолетних, уголовно-правовое предупреждение, цифровая виктимность несовершеннолетних

A. V. Mayorov
doctor of Law, Associate Professor
Ural State Law University named after V. F. Yakovlev

Criminal law prevention of digital victimity of minors

Abstract. The article is devoted to the analysis of modern trends in the field of digitalization and its impact on the interaction and life of people, with a special emphasis on the problems associated with the use of Internet resources by minors. The author considers the large-scale introduction of digital technologies based on artificial intelligence and software products that are actively transforming traditional forms of communication and life, especially in the context of social networks and instant messengers, the most popular among teenagers and young people. The central topic of the study is the issue of the low level of digital and information protection of minor users, which is directly related to the growth of digital victimization among this catego-

ry of the population, as well as the necessary criminal law protection. The criminal law mechanism for reducing the digital victimization of minors is considered.

Keywords: victimization, victimization of minors, criminal law prevention, digital victimization of minors

Введение. В современном мире сохраняется тенденция к замещению традиционных форм взаимодействия и жизнедеятельности людей интернет-ресурсами. Так, в нашу жизнь активно внедряются цифровые технологии, используемые искусственный интеллект и различные программные продукты. Масштабное развитие онлайн-индустрии способствует появлению новых форм цифрового взаимодействия на различных цифровых платформах. При этом ведущее место продолжают занимать социальные сети и мессенджеры, в первую очередь среди лиц, не достигших возраста 18 лет, и молодежи в целом. Особую обеспокоенность в связи со стремительным развитием интернет-среды вызывает низкий уровень цифровой и информационной защиты пользователей, чаще всего как раз несовершеннолетних, что и приводит в последующем к развитию цифровой виктимности несовершеннолетних.

Основная часть. В широком социологическом значении процесс цифровизации ученый определяет как широкомасштабное внедрение информационных цифровых технологий во все сферы социальной реальности, жизни и деятельности человека. Цифровизация оказывает колоссальное влияние на основные подсистемы социума (экономику, политику и управление, образование, культуру и массмедиа, здравоохранение), на социальную структуру общества («цифровая стратификация») и его функционирование, вызывая новые социальные, коммуникативные, девиантные эффекты и практики [1. С. 33].

Более того, развитие цифрового пространства, помимо возникновения угрозы вовлечения несовершеннолетних в преступную и антиобщественную среду, представляет для злоумышленников дополнительные возможности, в виде распространения широкого круга деструктивных идей, не имеющих конкретного адресата, что в последующем приводит к потенциальному приобщению несовершеннолетних к такого рода негативным установкам в виде самостоятельного совершения ими в будущем единичного или группового преступления, т. е. общему росту преступности среди лиц, не достигших возраста 18 лет.

Медиапространство, а равно цифровая среда, независимо от словоупотребления, имеют ряд существенных особенностей, который отражает сущность данной системы в совокупности с ее структурными компонентами, в том числе формируя предпосылки для вовлечения несовершеннолетних в сети.

Во-первых, виртуальная зона взаимодействия субъектов включает в себя различные формы содержания информации, например, конкретные медиаплатформы, социальные сети, сетевые программы, цифровые порталы, информационно-коммуникационные каналы связи и т. п. Следовательно, медиапространству, как и всему виртуальному миру, присущи определенные способы конфигурации данных, посредством которых реализуется работа с информацией и взаимодействие этих субъектов между собой.

Во-вторых, любая цифровая среда подвержена стремительному развитию и усовершенствованию с учетом ежедневной разработки современных инновационных технологий, методов цифрового воздействия и расширения каналов коммуникации в рамках единого информационного поля.

В-третьих, медиапространство характеризуется отсутствием единой целевой аудитории, в связи с наличием широкого объема информации. Следовательно, оно является доступным для каждого, что приводит к объективному увеличению числа пользователей в сети, и в последующем может существенно затруднять при необходимости их идентификацию в цифровых порталах.

В-четвертых, информационная среда в большинстве случаев не отвечает должному уровню защиты данных ввиду наличия постоянного процесса оптимизации медиаресурсов, а равно создания злоумышленниками новых каналов, позволяющих обойти систему безопасности сетевой платформы.

В-пятых, в связи с большим объемом используемой и хранящейся в базах информации, любое медиапространство несет в себе потенциальную, а чаще реальную угрозу утечки данных. Подобное означает, что каждая интегрируемая в сетевое поле цифровая площадка создает риск хищения персональной информации или совершения иного противоправного деяния в отношении обычных пользователей.

По результатам проведенного нами социального опроса, более 89% респондентов (несовершеннолетних) проводят свободное время в Интернете. Среднее времяпрепровождение составляет не менее трех часов в день, а первое использование гаджетов и выход в Интернет осуществляются ими уже по достижению возраста 6-7 лет. Указанные обстоятельства приводят к возникновению повышенного уровня уязвимости детей в медиапространстве, с точки зрения их возможного вовлечения в преступную или антиобщественную среду и, как следствие, приобщение к деструктивным установкам.

Совершение преступлений с использованием цифровых технологий уже очевидный факт, количество этих преступлений в последние годы получило широкое распространение. Свидетельством этому является официальная статистика количества зарегистрированных преступлений в России, данные, полученные от организаций, осуществляющих кибербезопасность и мнение их экспертов. Это еще раз убеждает в том, что изменения происходят не только в обществе, меняется и преступность, появились малоизученные способы и средства совершения преступлений, в частности преступления, совершаемые в сфере цифровых технологий или с их использованием (цифровая преступность, преступления в сфере цифровых технологий включают в себя преступления, совершаемые в сфере высоких технологий с использованием информационно-телекоммуникационных технологий) [2. С. 150].

Всего за январь–июль 2025 г. в России было зарегистрировано 424,9 тыс. правонарушений, совершенных с применением ИТ-инфраструктуры или в сфере компьютерной информации. Из них свыше 355 тыс. были совершены в интернете. По данным МВД, число киберпреступлений в онлайн-среде увеличилось на 2,2% по сравнению с аналогичным периодом 2024 года.

Несмотря на положительные тенденции в части раскрываемости, в министерстве подчеркивают, что цифровая преступность остается устойчиво тяжелой по своей структуре. Более трети от всех зарегистрированных преступлений в стране так или иначе связаны с использованием цифровых каналов.

При этом на фоне общего снижения темпов роста преступности, доля ИТ-преступлений продолжает оставаться высокой – более 33% от всех зарегистрированных инцидентов.

При этом в ведомстве подчеркивают, что расследование цифровых преступлений осложнено рядом системных проблем. Одной из них называют отсутствие законодательных норм, что способствует уходу преступников от ответственности [6].

Среди наиболее опасных видов преступлений, совершаемых в указанных сферах, можно выделить:

– ст. 2052 УК РФ «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма» (+57%);

– ст.2281 УК РФ «Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества» (+73,2%);

– ст.242, ст.2421, ст.2422 УК РФ «Изготовление порнографических материалов» (–1,3%);

– ст.273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» (+77,9%);

– ст.280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности» (+53,5%).

Эти обстоятельства, безусловно, свидетельствуют о повышенном влиянии медиапространства на жизнь и безопасность людей, в особенности несовершеннолетних, в контексте совершения широкого спектра противоправных деяний в информационной среде (киберпреступлений).

Цифровая виктимизация включает в себя весь спектр противоправных деяний, распространенных в физическом мире, ученые-криминологи часто обсуждают, понимают и рассматривают ее по-разному, потому что правонарушения совершаются без физического взаимодействия жертвы и правонарушителя (например, домогательства, сексуальные домогательства, преследование).

Так в исследовании Д.Д. Медведева приходит к выводу, что среди основных угроз, возникающих в информационной среде и непосредственно, представляющих опасность для несовершеннолетних с учетом использования последними всего масштаба имеющихся медиаресурсов, в том числе сети Интернет, следует учитывать:

– «распространение личных данных пользователей (видео, фотографии и т. д.) с учетом их последующего похищения злоумышленниками, например, ввиду разработки и внедрения вредоносных компьютерных программ;

– распространение порнографических материалов в целях посягательства на моральную основу общества, в частности, нравственное развитие несовершеннолетних;

– распространение и (или) употребление наркотических веществ, а также алкоголя либо приобщение к иным вредным привычкам, например, токсикомании, в силу пропаганды среди молодежи нездорового образа жизни;

– вовлечение несовершеннолетних в реализацию незаконных схем вывода денежных средств (мошенничество и т.п.) как результат неправомерного обогащения или быстрого заработка (эффект «легких» денег), что представляет особый интерес для лиц, не достигших возраста 18 лет;

– вовлечение несовершеннолетних в деструктивные движения, опасные для жизни и здоровья последних (руфинг, зацепинг и т.д.) ввиду стремления обратить на себя внимание взрослых или заполучить авторитет среди сверстников;

– популяризация среди несовершеннолетних суицидальных форм поведения, с учетом окончательно несформированной психики подростков;

– вовлечение несовершеннолетних в занятие проституцией;

– распространение идей экстремистского и террористического толка на фоне отсутствия должного уровня правосознания у детей;

– кибербуллинг» [5. С. 71].

Последнее, в частности, на современном этапе развития общества все чаще внедряется в повседневную жизнь и становится особенно популярным среди молодежи. При этом общий уровень проблематики роста данного негативного явления связывается не только с усовершенствованием возможностей информационной среды, но и внутренними особенностями личности [4. С. 176]. Например, в виде проявления неконтролируемой агрессии, травли, жестокости или публичных издевательств, каждое из которых носит психотравмирующий характер в отношении конкретного субъекта или нескольких лиц. Именно эти факторы в последующем создают предпосылки для уязвимости несовершеннолетних в сети, поскольку реализация злоумышленниками подобных форм девиантного поведения в цифровой среде может выступать одним из условий успешного вовлечения лиц, не достигших возраста 18 лет, в деструктивные движения, ввиду оказания на них жесткого эмоционального воздействия неизвестным пользователем в Интернете.

Таким образом, можно прийти к выводу, что медиапространство как одна из самых распространенных площадок вовлечения несовершеннолетних в противоправную деятельность на сегодняшний день характеризуется следующими признаками, отражающими низкий уровень защищенности детей в сети и повышающими уровень их цифровой виктимности:

– высокая степень анонимности в сети, которая чаще всего ведет к невозможности установления личности виновного или конечного исполнителя с учетом реализации вовлечения несовершеннолетнего группой лиц;

– широкий спектр используемых виновным каналов вовлечения несовершеннолетних, в том числе, таких как средства массовой информации, Интернет-ресурсы, спам-рассылки, сетевые и онлайн-игры и т.п., вследствие чего

сложно заранее спрогнозировать, какую форму воздействия выберет преступник в следующий раз;

– возможность подмены преступником своей социальной роли и возраста, в виду чего несовершеннолетний может воспринимать виновного как друга или знакомого и не подозревать о реальном возрасте, половой принадлежности и социальной роли виновного, а равно об осуществлении в отношении него процесса вовлечения как такового;

– неограниченный перечень способов вовлечения несовершеннолетних в преступную среду, в виду чего формы взаимодействия виновного и потерпевшего могут существенно отличаться в каждом конкретном случае, что, в свою очередь, затрудняет возможность выработки унифицированного подхода в рамках профилактической и предупредительной работы по данному направлению;

– свободный доступ к личным данным в современном пространстве, в том числе в информационном поле, в сети Интернет, а также даже в малых группах среди сверстников или иного круга общения несовершеннолетнего, исходя из чего, не всегда можно установить, истинную мотивацию виновного – почему преступник выбрал именно эту, а не какую-либо другую жертву [3. С. 115].

Указанные факторы позволяют сделать вывод, что на современном этапе развития медиапространства с учетом наличия большого количества и доступности различных цифровых ресурсов, включая не только Интернет, как общую сферу дислокации таких площадок, но также и СМИ, телефонные сети, современные digital технологии, социальные сети и мессенджеры, печатные издания, визуальную рекламу, онлайн-порталы и блоги, нейросети и чат-боты, институт вовлечения несовершеннолетних в преступную и антиобщественную среду остается полноценно не защищенным. Интернет и социальные сети стали одним из величайших достижений современного общества, однако они также представляют собой одну из самых больших опасностей в отношении защиты персональных данных и прав человека, в частности, права на неприкосновенность частной жизни [8. С. 400].

Основными элементами низкого уровня безопасности лиц, не достигших возраста 18 лет, с учетом использования ими перечисленных выше способов получения информации, являются:

– несовершенство уголовно-правовых и иных законодательных средств воздействия;

– чрезмерная доступность медиаресурсов для детей;

– отсутствие должного уровня цифровой грамотности у несовершеннолетних;

– недостаточная техническая защита данных и цифровых систем;

– отсутствие осуществления необходимого контроля над информацией, публикуемой в сети, с учетом ее соответствия цензуре.

Так, несмотря на очевидное влияние сети Интернет на формирование личности несовершеннолетнего, а равно возможность его вовлечения в преступную или антиобщественную деятельность, законодатель только в текущем году, наконец, ввел ответственность за вовлечение лиц, не достигших возраста

18 лет, в противоправную деятельность посредством использования информационно-телекоммуникационных сетей (п. «б» ч.2 ст.150 УК РФ, ст.151 УК РФ) [7].

При этом ч. 3 данных норм предусматривает ответственность за указанное деяния, совершенное с применением насилия или угрозой его применения (п. «а»), в отношении двух и более лиц (п. «б»), в отношении лица, не достигшего четырнадцатилетнего возраста (п. «в»).

В ч. 4 ст. 150 УК РФ диспозиция предусматривает ответственность не только за вовлечение в совершение преступлений различной степени тяжести (пп. «б», «в»), но и в преступную группу (п. «а»), а также в совершение преступления по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы (п. «г»).

До недавнего времени осуществляемая в сети злоумышленниками преступная деятельность в контексте вовлечения несовершеннолетних не охватывалась рамками закона, что, безусловно, считалось огромным упущением, поскольку интересы и права детей не защищались должным образом, а виновные оставались безнаказанными.

Однако стоит отметить, что введенная законодателем норма об уголовной ответственности за вовлечение несовершеннолетних в сети, хотя и явилась важным достижением в нормативном регулировании данного института, но в полной мере все же не обеспечивает безопасность физических лиц.

В первую очередь, это связывается с отсутствием должных механизмов выявления такого рода преступлений в реальной жизни. Иными словами, уровень киберпреступников, а равно разрабатываемых ими способов совершения указанных противоправных деяний не совпадает со степенью защиты медиаресурсов, с точки зрения, обеспечения безопасности, как самой системы, так и ее пользователей.

Степень подготовки технических специалистов не отвечает в полной мере реализации задач по борьбе с цифровой преступностью, поскольку факторов сдерживания информационных рисков и угроз намного меньше, чем создаваемых виновными путей и каналов обхода системы защиты компьютера или цифровых сетей в целом.

Подводя итог, необходимо подчеркнуть, что развитие информационных технологий и цифрового поля в целом позволяют достичь высоких результатов в контексте модернизации методов общения людей, реализации ими удаленного доступа к различным ресурсам без территориальных и временных ограничений, возможности организовывать дистанционно свою профессиональную деятельность и т. д.

Однако подобный прогресс имеет также существенные недостатки, в частности, указанные достижения в области информационного и цифрового права предопределили смещение вектора преступных намерений виновных лиц в сторону их проявления в виртуальной среде с учетом использования телекоммуникационных каналов, в том числе сети Интернет.

При этом любые незаконные деяния, осуществляемые в сети или с использованием таких информационных технологий, а равно ответственность, за которые прямо предусмотрена действующим законодательством, получили персональное название «киберпреступность», что подчеркивает масштаб их распространения и спектр неопределенного круга лиц, являющихся потенциальными жертвами указанной категории противоправных деяний.

Заключение. Все вышеперечисленное обуславливает объективный рост числа преступлений, совершаемых в информационной среде, в большей степени в отношении несовершеннолетних. В частности, институт вовлечения лиц, не достигших возраста 18 лиц, приобретает с каждым днем новые характерные черты, значительно отличающие его от «простого» вовлечения, реализуемого виновным при непосредственном личном контакте с потерпевшим.

Во-первых, увеличивается общая аудитория несовершеннолетних, использующих в повседневной жизни различные гаджеты, иные цифровые устройства, в том числе с расчетом на осуществление выхода через указанные системы в Интернет пространство.

Во-вторых, конфигурация данных в сети предполагает высокую степень виктимности каждого подростка с учетом доступности медиаресурсов в настоящее время.

В-третьих, в связи с ежедневным использованием Интернет-ресурсов попытки справиться с регулярно растущим потоком информации значительно снижаются, это приводит к возникновению психического дисбаланса, стрессу и общему перенапряжению, что снова делает ребенка более уязвимым для злоумышленника.

В-четвертых, у несовершеннолетних отсутствует полноценная возможность внутренней саморегуляции и контроля за времяпрепровождением в сети, а равно контроля за выбором источников информации, медиаплатформ и т.п., поскольку большинство из них обращает внимание на интересный контент, привлекательные фразы, яркие рекламы и не следит за безопасностью собственных данных.

В-пятых, вовлечение как целостное негативное явление с учетом его проявления в цифровом пространстве, на практике, как мы отмечали ранее, очень трудно выявить, что приводит к тому, что такие преступления, остаются латентными, а виновный или конечный исполнитель сохраняют свою анонимность и продолжают реализовывать преступные мотивы в отношении еще большего круга несовершеннолетних лиц.

Однако стоит отметить, что введенная законодателем норма об уголовной ответственности за вовлечение несовершеннолетних в сети «Интернет», хотя и явилась важным достижением в нормативном регулировании данного института, но в полной мере все же не обеспечивает виктимную безопасность несовершеннолетних.

В первую очередь, это связано с отсутствием должных механизмов выявления такого рода преступлений в реальной жизни. Иными словами, уровень киберпреступников, а равно разрабатываемых ими способов совершения указанных противоправных деяний не совпадает со степенью защиты цифрового

пространства, с точки зрения, обеспечения безопасности, как самой системы, так и ее пользователей.

Цифровая виктимность несовершеннолетних продолжает зависеть от объективных рисков и угроз преступного воздействия, а действующая система уголовно-правовых и технических средств противодействия данным негативным явлением не способна в полной мере отвечать современным информационным вызовам, поскольку не успевает адаптироваться к новым и постоянно меняющимся противозаконным методам злоумышленников, что и представляет собой главную на сегодняшний день практико-ориентированную проблему.

Список литературы

1. Комлев Ю. Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии // Вестник Казанского юридического института МВД России. 2020. Т. 11, № 1. С. 31–40. DOI: 10.24420/KUI.2020.39.1.004
2. Майоров А. В. Влияет ли цифровизация на виктимизацию в современном обществе? // Виктимология. 2022. Т.9, №2. С. 148-156.
3. Медведева Д. Д. Криминологические аспекты совершения преступлений, предусмотренных ст. 150, 151, 151.1 и 151.2 УК РФ // Социальное управление. 2024. Т. 6, № 3. С. 111–119.
4. Медведева Д. Д. Несовершеннолетние как жертвы эмоционального и психологического насилия в современном обществе: проблема криминализации // Защита жертв преступлений в современном обществе (PVCMS 2023): материалы VI Международной научно-практической интернет-конференции, Челябинск, 21–22 февраля 2023 года. Челябинск: Общество с ограниченной ответственностью "Эскуэла", 2023. С. 172-179.
5. Медведева Д.Д. Вовлечение несовершеннолетних в совершение преступления или иную антиобщественную деятельность в сети Интернет: основные угрозы и группы риска // Вестник экономики, управления и права. 2025. Т. 18. № 1. С. 69-74. DOI: 10.47475/3034-4247-2025-18-1-69-74.
6. Почти 30% IT-преступлений в России не удается раскрыть. URL: https://cisoclub.ru/v-rossii-raskryvaemost-it-prestuplenij-dostigla-pochti-30-no-struktura-cifrovoj-prestupnosti-ostajotsja-slozhnoj/ (дата обращения: 20.09.2025).
7. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 14.02.2022) // Собрание законодательства РФ. 17 июня. Ч. 1 ст.150 УК РФ. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/7815cc725bea068c1487613dedc48408265c9636 (дата обращения: 20.09.2025).
8. Аранда Серна Ф.Х. Социально-правовые риски шерентинга в процессе формирования цифровой идентичности ребенка в социальных сетях // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 394-407. https://doi.org/10.21202/jdtl.2024.20. EDN: gbfhor.

УДК 343.2/.7

Э. С. Намазов,
аспирант,
Казанский (Приволжский) федеральныйо университет

Жертвы мошенничеств, вовлекаемые в преступления террористической направленности с использованием информационно-телекоммуникационных технологий: уголовно-правовой и виктимологический аспект

Аннотация. Статья посвящена анализу складывающейся практики совершения криминальных поджогов, квалифицируемых по ст. 167 (умышленное уничтожение или повреждение имущества) и ст. 205 УК РФ (террористический акт). Все чаще исполнителями преступлений выступают, лица, ставшие жертвами преступлений в сфере мошенничеств, вследствие чего под воздействием манипулятивного воздействия со стороны злоумышленников, находящихся за пределами России, совершают преступления, квалифицирующиеся как террористический акт (поджоги военкоматов, железнодорожных релейных шкафов). Приведена актуальная правоприменительная практика совершения криминальных поджогов; продемонстрирован механизм вовлечения в преступную деятельность виктимизированных лиц, находящихся после совершения преступления в фрустрированном состоянии, и совершения ими последующих преступлений. Даны рекомендации по профилактике совершения криминальных поджогов жертвами преступлений: информационно-просветительская работа среди населения, виктимологическое сопровождение и психологическая помощь жертвам преступлений.

Ключевые слова: криминальные поджоги, умышленное уничтожение или повреждение имущества, террористический акт, жертва преступления, виктимизация

E.S. Namazov,
Kazan (Volga Region) Federal University, Kazan, Russian Federation

Victims of fraud involved in terrorism-related crimes using information and telecommunication technologies: a criminal law and victimological perspective

Abstract. This article is dedicated to the analysis of the emerging practice of committing criminal arson, classified under Article 167 (intentional destruction or damage to property) and Article 205 of the Criminal Code of the Russian Federation (terrorist act). Increasingly, the perpetrators of these crimes are individuals who have become victims of fraud, who, under the manipulative influence of assailants located outside of Russia, commit acts classified as terrorist offenses (such as the arson of military enlistment offices and railway relay cabinets). The article presents current

law enforcement practices regarding criminal arson; it demonstrates the mechanism through which victimized individuals, after committing a crime, find themselves in a state of frustration and subsequently engage in further criminal activities. Recommendations are provided for preventing criminal arson by crime victims, including informational and educational outreach to the public, victimological support, and psychological assistance for victims of crime.

Keywords: criminal arson, intentional destruction or damage of property, terrorist act, victim of a crime, victimization

Введение. Проблема терроризма остается на сегодняшний день одной из самых сложных социальных негативных явлений в различных ее проявлениях и формах. Вызывают серьезные опасения происходящие в мире тенденции, которые выражены в совершениях террористических актов, расширении географии терроризма (стирание границ), сращивание террористических организаций с организованной преступностью, вовлечение в террористическую деятельность, популяризацию терроризма с помощь новых информационных технологий и коммуникаций, распространение радикальной идеологий. Перечисленные явления ведут к межэтническим и религиозным конфликтам, и, как следствие, провоцирует нестабильную обстановку как регионе, так и в стране в целом, смену легитимных режимов с помощью «цветных революций», локальные и региональные войны, которые приводят к бессмысленным многочисленным жертвам среди мирного населения.

Основная часть. Уровень террористической угрозы в России по состоянию на 2025 год согласно глобального индексу терроризма, равен 6,267 по рейтингу из 237 стран. Россия занимает 16 место (первую десятку занимают такие страны как Пакистан, Сомали, Сирия, Израиль, Афганистан) [1].

По данным ГИАЦ МВД России за 2010-2024 гг. было совершено преступлений террористического характера в 2010 г. – 581, 2011 г. – 622, 2012 г. – 637, 2013 г. – 661, 2014 г. – 1128, 2015 г. – 1538, 2016 г. – 2227, 2017 г.- 1871, 2018 г. – 1679, 2019 г. – 1806, 2020 г. – 2342, 2021 г. – 2136, 2022 г. – 2233, 2023 – 2382, 2024 – 3714 [2]. В обществе каждое такое преступление вызывает широкий общественный резонанс.

В 2024 г. зарегистрирован рекордный показатель терактов – 1191 (в 2023 – 410, в 2015 – 8) [3]. Рост совершения террористических актов начался в 2022 году. Это связано с расширением террористической активности, когда правоохранительные органы все чаще квалифицируют как террористический акт действия, связанные с поджогами военкоматов, железнодорожных релейных шкафов, военной техники, а также использование БПЛА, в террористических целях.

Проявление терроризма обусловлено обострением социальных конфликтов общества экономической ситуацией в стране, социального неравенства, безработицей, коррупцией, обесцениванием духовных и культурных ценностей, нигилизмом, низкой правовой культурой, распространения радикальных взглядов и идей, обосновывающих агрессию, насилие и нетерпимость.

Цифровизация общества повлияла на трансформацию системы общественных отношения. Развитие общества перешло на новый качественный

научно-технический уровень. Информационные технологии приобрели, глобальный характер присутствуют во всех сферах жизнедеятельности общества и государства. На цифровые технологии завязаны многие виды деятельности человека и осуществления государственных функций. Сегодняшний мир неизбежно уходит в Интернет, электронные или информационно-телекоммуникационные сети. Государства стремиться усилить контроль за Интернет-пользователями, данная проблема является одной из задач правоохранительных органов, которые на постоянной основе проводят специальные мероприятия по веб-сайтам, адресам электронной почты, мессенджеров, социальных сетей, Даркнету и др., лиц и организаций, оказывающих финансирование террористам. Контролем Интернета в России занимаются специальные службы ФСБ России, ЦПЭ МВД России, прокуратура и Роскомнадзор. Принят ряд законодательных актов, позволяющих вести наблюдение за Интернетом, большинство из которых направлены на блокировку доступа. Необдуманное и невзвешенное вмешательство государства в эти процессы могут нанести серьезный урон свободе информации и ограничение свободы слова. Современные процессы глобализации мира сужают значимость государственных границ, международный терроризм не стал исключением в развитии глобализации. Террористические организации, отдельные фанатики, лица с психическими отклонениями, организованные преступные группы активно применяют информационно-телекоммуникационные сети Интернет (медийное пространство), в своих противоправных целях (пропаганда, агитация, вовлечение, руководство к действию, координация преступной деятельности), для поддержания культа насилия, националистических идей фашистского толка или «глобального джихада». Долгое время феномен терроризм воспринимался лишь как материальные акты насилия, в действительной реальности очень быстро развиваются виртуальные преступления, среди которых отдельно можно выделить кибертерроризм, информационный терроризм, в ближайшем будущем, терроризм с использованием искусственного интеллекта (ИИ), а также спутниковый или космический терроризм.

С феноменом поджогов российское общество столкнулось после начала Специальной военной операции на территории Украины (февраль 2022 год), когда злоумышленники вовлекают или заставляют российских граждан, связанных с мошенническими действиями, совершать преступления террористической направленности в виде поджогов военкоматов, административных зданий, иных форм вандализма и т.д., с ярко выраженными политическими и экстремистскими мотивами. С другой стороны, ведется планомерная работа заинтересованных лиц, через различные социальные сети, мессенджеры, Даркнет, в вовлечении в совершение терактов за денежное вознаграждение, так называемый феномен «спортиков».

Суть феномена («спортиков») в том, что заказчик преступления, находит исполнителей посредством мессенджеров, социальных сетей, Даркнет, вблизи объекта преступления (военная или гражданская инфраструктура), в отношении которого совершается поджог, теракт или применяют физическое насилие за денежное вознаграждение.

Статья 167 УК РФ размещена в УК РФ в Разделе VIII в Главе 21 «Преступления против собственности», а статья 205 УК РФ в Разделе IX в Главе 24 «Преступления против общественной безопасности».

Непосредственным объектом ст. 167 УК РФ являются отношения против собственности. Предмет выступает чужое имущество. Объективная сторона преступления выражается в умышленном уничтожении чужого имущества, если деяние приняло значительный ущерб, которое определяется из имущественного положения потерпевшего [4]. Субъективная сторона – прямой умысел. Субъект вменяемое физическое лицо, достигшее 16 возраста, а по ч. 2 ст. 167 УК РФ – с 14-летнего возраста.

Родовым объектом ст. 205 УК РФ является общественный порядок, который направлен на поддержание общественного спокойствия.

С объективной стороны террористический акт ст. 205 УК РФ может совершаться двумя альтернативными способами: 1) совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели людей человека, причинение значительного имущественного ущерба либо наступление иных тяжких последствий и 2) угроза совершения указанных действий [5. С. 464; 6. С. 375].

Субъект ст. 205 УК РФ признается вменяемое физическое лицо, достигшее 14-летнего возраста. Субъективная сторона террористического акта характеризуется прямым умыслом и специальной целью дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений – на это обращает внимание пункт 1 Постановления Пленума Верховного суда РФ от 09.02.2012 № 1 [7]. При отсутствии специальной цели квалификация по ст. 205 УК РФ исключается.

В настоящее время отсутствуют разъяснения Верховного Суда Российской Федерации по вопросу единообразного применения законодательства Российской Федерации, в части квалификации поджогов военкоматов и административных зданий.

Важнейшей тенденцией прослеживающийся в характеристики деяний лиц, совершающих преступления, сопряженные с поджогами чужого имущества, выступает активная предшествующая виктимизация лиц, совершающих данные преступления. В широком смысле, под жертвой в современной виктимологии понимается лицо, понесшее вред от любого последствия совершенного противоправного деяния [8. С. 38]. Анализ складывающейся правоприменительной практики показывает существование порочного круга, когда жертва, пострадавшая от той или иной формы противоправного поведения, сама вовлекается в совершение преступлений, порождая порочный круг становления пострадавшего преступником, деяния которого влечет появление новых жертв и новых преступников соответственно. Наиболее ярко данная закономерность прослеживается в совершении криминальных поджогов, квалифицируемых по статьям, устанавливающим ответственность за преступления против собственности, либо против общественной безопасности, совершаемых лицами пострадавшими от вовлечения в наркопотребление (жертвы наркотизма в широком смысле слова) и потерпевшими от мошенничества.

Преступления против собственности, как показывает современная практика, также приводят к тому, что жертвы подобных преступлений попадает в группу риска, подверженную манипулированию в целях подталкивания ее к совершению посягательств на имущество граждан и общественную безопасность, посредством совершения поджогов. В литературе отмечается, что «собственные личные ресурсы [жертвы преступления] существенно умалены преступлением» [9. С. 66]. Жертвы преступлений особенно уязвимы к вовлечению противоправную деятельность, поскольку их фрустрированное состояние, зацикленность на собственных негативных переживаниях снижает критику происходящих событий. Психологически дестабилизированное вследствие совершения преступления лицо, последует указаниям манипулятора тогда, когда лицо, не находящееся в стрессовой ситуации, будет невосприимчиво к подстрекательству в совершении преступления.

К специфическим способам вовлечения в совершение рассматриваемого преступления на фоне проводимой СВО можно отнести мошенничество и шантаж. Лица до совершения ими преступления, подвергались психологической обработке со стороны заинтересованных лиц (зарубежных спецслужб), последние заставляют и убеждают своих жертв под предлогом возврата ранее похищенных мошенническим способом денежных средств или угроз физической расправы в отношении близких родственников, поджигать административные здания исполнительной власти или социальные объекты инфраструктуры, иногда злоумышленники заставляли своих жертв выкрикивать антивоенные или проукраинские лозунги.

Приведем три примера из правоприменительной практики. В примере № 1, описано вовлечение лица в преступление поджог военкомата, путем угроз, в отношении которого ранее были совершены противоправные действия (ч. 4 ст. 159 УК РФ). В примере № 2, описано вовлечение лица, в преступление поджог административного здания, путем убеждений (идеологии). В примере № 3, описаны действия лиц, совершивших поджог входной двери жилого дома за денежное вознаграждение.

Пример № 1. В период с 29 по 31 июля 2023 года в Российских регионах совершена целая серия поджогов военкоматов. В Республике Татарстан г. Казани в указанный период было совершено более четырех попыток поджогов военкоматов. Так, 25.07.2023 в отношении жительницы г. Казани были совершены мошеннические действия со стороны неустановленных лиц, которые представлялись сотрудниками силовых структур России, А., 1961 г.р., оформила кредит в пяти банках и перевела дистанционно злоумышленникам 2 200 000 рублей. В полицию она по факту мошенничества не обращалась. 29.07.2023 около 22 час. 00 мин. с А., по сотовому телефону вновь связалось неустановленное лицо, представившись сотрудником правоохранительных органов, которое стало угрожать физической расправой ее дочери, проживающей в другом городе, заставило совершить поджег военкомата. По указанию неустановленного лица А., купила 3 литра бензина на заправке, далее направилась в сторону военкомата. 29.07.2023 в 23 час. 20 мин. А., находясь в эмоциональном подавленном состоянии, выполнила требования злоумышленника, облила фасад зда-

ния военного комиссариата Кировского и Московского районов г. Казани горючей жидкостью и подожгла ее, в результате чего произошло возгорание площади 17,07 кв.м. В момент поджога женщина общалась с неустановленным лицом по видео-звонку. Преступные действия А., были пресечены сотрудниками полиции, очаг возгорания ликвидирован. По данному факту следственным органом возбуждено уголовное дело по ч. 3 ст. 30, ч. 2 ст. 167 УК РФ [14. С. 195]. После проведения ряда судебных экспертиз уголовное преследование в отношении А., было прекращено, в виду того, что она была под воздействием третьих лиц.

Пример № 2. 24.01.2025 в 14 часов 35 минут неустановленное лицо совершил поджег административного здания порохового завода по адресу: г. Казань, ул. 1 Мая. В средствах массовой информации сообщалось, что молодой человек попытался поджечь, а именно кинул на крыльцо смесь по типу «Коктейль Молотова» [10].

24.01.2025 СЧ СУ УМВД России возбуждено уголовное дело №12501920008000007 по ч. 1 ст. 205 УК РФ. Материалы уголовного дела переданы в первый отдел по расследованию особо важных дел СУ СК России по Республике Татарстан.

31.01.2025 путем оперативно-розыскных мероприятий сотрудниками отдела уголовного розыска УМВД России по г. Казани задержан Р., 2008 г.р. (16 лет), учащегося 10-го класса одной из среднеобразовательных школ города. В отношении несовершеннолетнего Вахитовским районным судом Казани избрана мера пресечения в виде заключения под стражу. В ходе допроса обвиняемый частично признал вину, пояснив, что таким образом решил доставить неприятности собственному отцу, который недавно ушел из семьи [11].

Проведенным осмотром средств связи, находящихся в пользовании у Р., 2008 г.р. обнаружен файл «Рецепты по майдановски» (на Украинском языке) с вариантами изготовления коктейля «Молотова». А также способы изготовления дымовых шашек, напалма. Кроме того, установлен удаленный чат мессенджера «Telegram» под названием «Клуб ликвидированных мотоблоков», состоящий из 7 пользователей. В указанном чате публиковались националистические изображения (свастика), а также украинская памятка «Инструкция по Майдановски». Из показаний свидетелей следует, что Р., 2008 г.р. придерживался националистических взглядов, ранее высказывал идею создать националистическую группу «правое движение на районе».

Пример № 3. 12.01.2025 в 17 часов 40 минут в отделе полиции № 17 «Ямашевский» УМВД России по г. Казани поступило сообщение, что в 16 часов 00 минут по адресу: г. Казань, ул. Мусина, дом ** квартира *, двое неизвестных мужчин подожгли общую тамбурную дверь на этаже много этажного жилого дома горючей смесью, заявитель Н., 1961 г.р.

В ходе проведенных мероприятий задержаны К., 1993 г.р., Г., 1997 г.р. которые пояснили, что нашли работу в «Telegram- канале», за поджег получили денежное вознаграждение 15 000 рублей.

В ходе дальнейшей проверки установлено, что общая дверь на три квартиры, в одной из квартир проживал Щ., 2002 г.р. которому 20.11.2024 был избрана мера пресечения в виде ареста обвиняемый по ч. 4 ст. 228.1 УК РФ.

По данному факту вынесено постановление об отказе в возбуждения уголовного дела по ч. 1 ст. 167 УК РФ. Тамбурную общую дверь установлена незаконно, собственник двери умер. Задержанные гр. К., 1993 г.р., Г., 1997 г.р. привлечены к административной ответственности по ст. 6.9 КоАП РФ.

В настоящее время сложилась негативная практика позволяющая уйти от наказания виновным лицам, ввиду малозначительности.

Преступные действия таких лиц, при поджогах дверей в жилых домах полагаем необходимо квалифицировать действия исполнителей по ч. 3 ст. 30, пп., «е», «ж», «з», «и», «л», «о» ч. 2 ст. 105 УК РФ, а организаторов по ст. 33 п. «з» ч. 2 ст. 105 УК РФ.

При поджогах административных зданий, объектов военной инфраструктуры квалифицировать по п. «в» ч. 2 ст. 205 УК РФ, а организаторов по ст. 33, ст. 205 УК РФ.

23.01.2025 в ходе итоговой коллегии МВД по Республики Татарстан глава ведомства генерал-лейтенант полиции Д.Р. Сатретдинов сообщил, что общий ущерб от киберпреступности за 12 месяцев в 2024 году в Республики Татарстан составил 5 млрд 773 млн 108 тысяч рублей, всего по России 168 млрд. [12].

Из-за активности мошенников Роскомнадзор и Минцифры обсуждали запрет на голосовые вызовы в мессенджеры (варианты блокировок: только на звонки из-за границы и полный запрет вызовов через мессенджеры [13]). В настоящее время пользователи социальных сетей испытывают трудности в общении с использованием мессендежеров (например, WhatsApp, Telegram).

Мы считаем, что законодателю не нужно принимать меры по ограничению Интернета в целях обеспечения безопасности. В качестве более эффективного направления профилактики вовлечения граждан в совершение криминальных поджогов мы предлагаем повышение правовой культуры население посредством широкой компании, направленной на информирование потенциальных жертв о способах совершения преступлений. Также полагаем необходимым осуществлять индивидуальное виктимологическое сопровождение потерпевших от преступлений, разъяснением им рисков от криминальной активности, предупреждение о возможном манипуляционном воздействии со стороны злоумышленников, оказанием психологической помощи и реабилитации.

Заключение. Правоприменителям же необходимо ориентировать на применение в отношении жертв преступлений, вовлеченных в криминальную деятельность, по возможности преимущественно уголовно-правовых мер альтернативного характера и назначения им наказания, не связанного с лишением свободы. Уголовно-правовая репрессия, по нашему мнению, должна быть в первую очередь направлена на лиц организующих совершение криминальных поджогов, и лишь по остаточному принципу на исполнителей, самих пострадавших от совершения преступлений.

Список литературы

1. Глобальный индекс терроризма 2019 / Рейтинг стран мира по уровню терроризма. URL: http://gtmarket.ru/ratings/global-terrorism-index (дата обращения: 18.09.2025).

2. Генеральная прокуратура РФ. Портал правовой статистики. URL: http://crimestat.ru/offenses_map

3. В 2024 году в России зафиксировано рекордное количество террористических актов // AVIA.PRO: URL: https://https://avia.pro/news/v-2024-godu-v-rossii-zafiksirovano-rekordnoe-kolichestvo-terroristicheskih-aktov?ysclid=mf8cnht5hx81756542 (дата обращения: 18.09.2025).

4. пункт 24 Постановление Пленума Верховного суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» // Справочно-правовая система «Консультант Плюс». URL: http://consultant.ru (дата обращения: 18.09.2025).

5. Уголовное право России. Особенная часть: учебник / под ред. Ф.Р. Сундурова, М.В. Талан, И.А. Тарханова. 2-е изд., перераб. и доп. М., Проспект, 2020, 992 с.

6.Наумов А.В. Российское уголовное право: Курс лекций. Т.2. Общая часть. М.: Юридическая литература, 2004. 832 с.

7. Постановление Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности»// Справочно-правовая система «Консультант Плюс». URL: http://consultant.ru (дата обращения: 18.09.2025).

8. Варчук Т.В. Вишневецкий К.В. Виктимология: учеб. пособие для студентов вузов, обучающихся по специальности «Юриспруденция» / Т.В. Барчук, К.В. Вишневецкий; под ред. С.Я. Лебедева. 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА: Закон и право, 2017. 191 с.

9. Будякова Т.П. Основы криминальной виктимологии: учебное пособие / Т.П. Будякова. 2-е изд., стер. Москва: ФЛИНТА, 2023. 88 с.

10. В Казани молодой человек пытался поджечь административное здание – его разыскивает полиция // Бизнес Online: [сайт]. URL: https://www.business-gazeta.ru/news/661088 (дата обращения: 15.03.2025).

11. МВД по РТ [сайт]. URL: https://t.me/mvdtatarstana/3280 (дата обращения: 18.09.2025).

12.Рустам Минниханов принял участие в расширенной коллегии МВД по Республики Татарстан // МВД по Республики Татарстан: [сайт]. URL: https://16.мвд.рф/news/item/60359315 (дата обращения: 18.09.2025).

13. Коллективная ответственность топ-мессенджеров // Коммерсант: [сайт]. URL: https://www.kommersant.ru/doc/7401636 (дата обращения: 18.09.2025).

14. Намазов Э.С. Поджоги военкоматов и административных зданий, совершенные на территории Российской Федерации: уголовно-правовая квалификация террористических актов // Правопорядок: история, теория, практика. 2024. № 4 (43). С. 191–200.

УДК 343.988

А. О. Синявина,
аспирант,
Казанский инновационный университет
имени В. Г. Тимирясова

Виктимологическая характеристика несовершеннолетней жертвы киберпреступности

Аннотация. Ежегодно количество киберпреступлений набирает немыслимый оборот, это прямо связано с развитием компьютерных технологий. Злоумышленники все чаще в качестве жертв выбирают несовершеннолетних, так как они в силу своих индивидуальных, социальных и психологических характеристикбольше подвержены угрозе стать обманутыми в киберпространстве. В Указе Президента Российской Федерации от 17.05.2023 № 358 «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года» закреплено, что защита прав и интересов детей в вопросах безопасного использования сети является основным приоритетным направлением работы государства в настоящее время. Поэтому целью настоящего исследования является выявление типичных виктимологических черт несовершеннолетней жертвы киберпреступности и предложение авторской формулировки понятия «кибервиктимность». Комплексное изучение виктимологической характеристики жертв указанной категории поможет составить программу профилактики и реабилитации виктимных подростков, а также это необходимо для формирования нормативно-правовой базы, которая будет зашивать права и интересы детей в киберсреде.

Ключевые слова: цифровые технологии, виктимологические черты, несовершеннолетние жертвы, кибепреступность, виктимология, кибервиктимология, ювенальная кибервиктимология

A. O. Siniavina,
Postgraduate Student,
Kazan Innovative University named after V. G. Timiryasov

Victimological characteristics of a minor victim of cybercrime

Abstract. Each year, the number of cybercrimes is reaching unprecedented levels, a trend directly correlated with the advancement of computer technologies. Malefactors are increasingly targeting minors as their victims, owing to their unique individual, social, and psychological characteristics that render them more susceptible to deception in cyberspace.

The Decree of the President of the Russian Federation No. 358 dated May 17, 2023, "On the Strategy for Comprehensive Child Safety in the Russian Federation for

the Period up to 2030" emphasizes that safeguarding the rights and interests of children in matters of safe internet usage is a top priority for the state at present.

Therefore, the primary objective of this research is to identify typical victimological traits of juvenile cybercrime victims and to propose an original author's definition of the concept of "cybervictimhood." A comprehensive study of the victimological characteristics of adolescent victims will facilitate the development of prevention and rehabilitation programs for victimized teenagers. Furthermore, this research is essential for establishing a normative legal framework to protect the rights and interests of children in the online environment.

Keywords: law, digitaltechnologies. victimologicaltraits, juvenilevictims, cybercrime, victimology, cyber victimology, juvenile cyber victimology

Введение. В соответствии с официальными статистическими данными в 2024 году в Российской Федерации совершено 765,4 тысячи IT-преступлений [16], это обусловлено невероятно быстрым ростом развития информационно-коммуникационных технологий и естественно дети и подростки подвержены преступным посягательствам в большей степени. По данным МВД России в 2024 году 95 843 детей стали жертвами всех преступлений [13]. «Информационное пространство несовершеннолетнего представляет собой информационно-коммуникативное поле его взаимодействия с другими участниками информационного социума, которое постепенно расширяется по мере взросления ребенка. Здесь следует говорить не только о взаимодействии несовершеннолетнего с различными источниками информации, но и о сложном процессе взаимодействия между всеми участниками (субъектами) информационных отношений, среди которых находится несовершеннолетний, что обуславливает необходимость изучения возможных рисков и угроз в данной сфере» – отмечает О.С. Рыбакова [11. С. 66].

Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» прямо закрепляет положения приоритетных направлений информационной безопасности Российской Федерации: «Развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия». «Обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий» [2].

«В современных условиях к основным угрозам безопасности детей относятся: распространение информации, представляющей опасность для детей, в том числе посредством информационно-телекоммуникационной сети "Интернет"» закреплено в Указе Президента Российской Федерации от 17.05.2023 № 358 «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года» [1]. Защита прав и интересов детей в вопросах безопасного использования сети является основным приоритетным направлением работы государства в настоящее время.

Дети более уязвимы перед киберпреступностью, чем взрослые, поскольку в силу возраста менее критично относятся к информации, получаемой в сети и

соответственно исследование типичных виктимологических характеристик несовершеннолетних жертв киберпреступлений необходимостью принятия и внедрения новых профилактических мер для их защиты и безопасного использования сети Интернет.

Целью настоящего исследования является выявление типичных виктимологических характеристик несовершеннолетней жертвы киберпреступности и предложение авторской формулировки понятия «кибервиктимность».

Для достижения поставленной цели были использованы теоретические методы, такие как анализ, синтез и обобщение.

Основная часть. Быстрое развитие информационно-коммуникационных технологий и способность каждого человека с помощью выхода в Интернет получить любую информацию в считанные секунды с одной стороны облегчает и улучшает качество жизни современного человека, а с другой стороны подвергает его огромной опасности и риску стать жертвой преступления в киберсреде.

Д.В. Жмуров определяет кибервиктимность как: «Способность индивида быть жертвой компьютерных преступлений в силу субъективной или объективной уязвимости» [8. С. 118]. А.Р. Дроздикова – Зарипова, Н.Н. Калацкая трактуют кибервиктимность как: «системное и динамичное свойство личности, проявляющееся в форме ее социального, биологического, психологического и морального деформационного отклонения, закрепленного в неосторожных, импульсивных, провоцирующих формах поведения, не соответствующего нормам безопасности и обусловливающего потенциальную или реальную предрасположенность субъекта становиться жертвой преступлений в глобальной сети Интернет» [7. С 161]. А.А. Батаева в своем исследование говорит, что: «Кибервиктимность – это способность стать жертвой преступления в Интернет-пространстве» [4. С. 90]. В продолжении исследований данных авторов предлагается авторская формулировка понятия «кибервиктимность» – это предрасположенность любого человека, не зависимо от возраста, и имеющего определенные физические, социальные и иные факторы стать жертвой преступления в киберсреде.

По данным МВД России, в 2024 году было совершено 84,8% преступлений с использованием интернета, это четыре из пяти [12]. Это свидетельствует о стремительном росте киберпреступности, и к большому сожалению, большой частью жертв становятся именно дети и подростки.

«К особым условиям виктимного поведения подростков, как правило, относят: персональный опыт или наблюдение фактов насилия, прежде выработанный набор психологических качеств (эмоциональная нестабильность, непостоянство, чрезмерное беспокойство, неудовлетворительное самомнение), недостаток социальной поддержки» [10. С. 58]. отмечают в своем исследовании авторы, а также выделяют следующие: «Это стремление проявлять независимость и самостоятельность, пренебрежение социальными нормами, тяга к риску, неумение оценивать свою безопасность, недостаточная сформированность осознанности, рефлексии, умения устанавливать связи между своим поведением и его последствиями, обобщать опыт» [6. С. 119]. «Слабость, неуравновешенность и инертность как базисные свойства виктимного подростка обуславливают проявление

таких личностных особенностей, как инфантильность застенчивость, робость, ранимость, которые в свою очередь, приводят к выработке адаптивной стратегии конформности, зависимости и отказу от своего Я» [3. С. 450-451].

На основе данных исследований можно сделать вывод, что, во-первых, виктимные черты подростков – это набор внешних и внутренних обстоятельств, таких как пережитый ими опыт и психологические переживания. А во-вторых, четко видна взаимосвязь личностных характеристик и предрасположенность к виктимизации. Такие черты подростка как эмоциональная нестабильность, неуверенность в себе, неумение оценивать риски и неспособность к пониманию своего поведения и ее анализу, а также к оцениваю рисков и последствий говорят о том, что несовершеннолетний стремится к самостоятельности, но пока не обладает набором определенных качеств и навыков для того, чтобы обеспечить себе защиту и безопасное использование Интернета.

«Рост мошеннической активности в отношении детей фиксируется нами с начала года как по собственной аналитике, так и по обращениям наших абонентов. Звонки мошенников блокируются, но многие злоумышленники общаются с детьми в соцсетях и мессенджерах. Одна из последних схем – вовлечение несовершеннолетних в преступную деятельность через предложения сдать свои аккаунты в мессенджерах и соцсетях в аренду за деньги. Такие учетные записи используются для мошеннических обзвонов, распространения вредоносного контента или проведения фишинговых атак, в том числе на друзей и знакомых через доверенные каналы общения. Кроме того, современные дети – продвинутые пользователи цифровых технологий и приложений, что делает их аккаунты особенно ценными для злоумышленников» [15], – считает директор департамента по предотвращению потерь доходов МегаФона Сергей Хренов.

Как отмечалось выше, подростки стремятся к самостоятельности и независимости, это сильно толкает их на изучение киберпространства, однако недостаток опыта и знаний делает их легкой добычей для преступников.

Рост кибермошенничеств в Российской Федерации связан с тем, что несовершеннолетие часто не знают, как вести себя в Интернете, они не могут знать популярные схемы мошенничества, такие как фишинговые сайты, «левые» аккаунты интернет-магазинов и прочее. Они часто с легкостью делятся личной информацией, переходят по ссылкам, не осознавая, в силу возраста, что подвергаются риску стать жертвой киберпреступления.

С начала 2025 года на детей пришлось на 30 процентов больше кибератак, чем в прошлом году. Об этом сообщают аналитики «МегаФона» и «Лаборатории Касперского». Преступники активно используют интерес школьников к играм, соцсетям и учебе, чтобы завладеть личными данными или деньгами родителей. [14]. К сожалению, данная тенденция характерна для всего современного мира, так как дети и их родители не в должной мере осведомлены о том, как можно защитить себя в интернете. А также в сочетании с отсутствием нормативных правовых актов, регламентирующих правовую защиту детей и подростов, создается благоприятная среда для совершения преступлений в киберпространстве.

А.Н. Берестовой отмечает: «Проблема виктимности детей и подростков в киберпространстве становится все более актуальной для России, поскольку им

доступны не только развлекательные сайты, но и запрещенные в РФ информационные порталы, которые могут оказывать негативное влияние на их психическое здоровье и социальное поведение» [5. С. 107]. «Семья, будучи ключевым звеном социальной адаптации детей и подростков, обладает значительным виктимогенным потенциалом» [9. С. 37]. По данным Mediascope: «Среди детей в возрасте от четырех до пяти лет интернетом пользуются 90 %. С возрастом этот показатель увеличивается и к 9–11 годам достигает 99 %. Ключевым устройством для выхода в интернет у детей и подростков остается смартфон: он есть у 77 % несовершеннолетних. Обходить блокировки дети умеют с раннего возраста: в группе от четырех до пяти лет 18 % пользуются VPN сами или с помощью взрослых» [17].

Отсюда следует сделать вывод, что родители, законные представители и опекуны обязаны следить за тем, как дети проводят время в интернете, посещают ли они запрещенные сайты в РФ уже с трехлетнего возраста, объясняя и показывая своим примером, как можно защитить себя и безопасно использовать киберсреду.

Заключение. Виктимологические черты несовершеннолетней жертвы киберпреступления – это набор личных, социальных и психологических факторов. Основные из них: эмоциональная нестабильность, неуверенность в себе, неумение оценивать риски и неспособность к пониманию своего поведения. Их совокупность обусловлена быстрым развитием информационно-коммуникационных технологий, изменением приоритетов у подростков и желанием как можно раньше начать использовать киберпространство. Комплексное изучение данных факторов поможет составить программу профилактики и реабилитации виктимных подростков. Также требуется формирование нормативно-правовой базы, которая будет прямо направлена на защиту прав и интересов несовершеннолетних в сети интернет.

Список литературы

1. О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года: Указ Президента РФ от 17.05.2023 № 358 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_ LAW_447320 (дата обращения: 15.09.2025).

2. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021№400 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 15.09.2025).

3. Базелюк В. В., Тыкман И. Р. Факторы виктимизации подростков в процессе социализации // Виктимология. 2024. № 3. URL: https://cyberleninka.ru/article/n/faktory-viktimizatsii-podrostkov-v-protsesse-sotsializatsii (дата обращения: 23.09.2025).

4. Батеева, А. А. Кибервиктимизация как проблема безопасности детей и подростков в современном социуме / А. А. Батеева // Социальная педагогика. 2020. № 4. С. 86–91.

5. Берестовой А.Н., Цветков П.В. О понятии и характеристике преступлений, совершаемых в отношении несовершеннолетних в киберпространстве // Вестник Санкт-Петербургского университета МВД России. 2023. №4 (100). URL: https://cyberleninka.ru/article/n/o-ponyatii-i-harakteristike-prestupleniy-sovershaemyh-v-otnoshenii-nesovershennoletnih-v-kiberprostranstve (дата обращения: 02.09.2025).

6. Бобченко Т. Г., Нефедова А. В. Психологический портрет личности виктимных подростков // Виктимология. 2025. №1. URL: https://cyberleninka.ru/article/n/psihologicheskiy-portret-lichnosti-viktimnyh-podrostkov (дата обращения: 23.09.2025).

7. Дроздикова-Зарипова А. Ф., Калацкая Н. Н., Валеева Р. А., Костюнина Н. Ю., Биктагирова Г. Ф. Социально-психологические особенности студентов, склонных к виктимному поведению в интернет-пространстве // Современные наукоемкие технологии. 2019. № 12-1. С. 159–166.

8. Жмуров Д. В. Кибервиктимность как новая категория виктимологии постмодерна // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. №2. URL: https://cyberleninka.ru/article/n/kiberviktimnost-kak-novaya-kategoriya-viktimologii-postmoderna (дата обращения: 03.09.2025).

9. Загуменных, М. А. Виктимность несовершеннолетних при вовлечении их в совершение антиобщественных действий / М. А. Загуменных, В. В. Денисович. Текст: непосредственный // Молодой ученый. 2021. № 33 (375). С. 36-38.

10. Петровских В.Д., Пенионжек Е.В. Склонность к виктимному поведению у подростков, особенности его проявления // Общество, право, государственность: ретроспектива и перспектива. 2023. №1 (13). URL: https://cyberleninka.ru/article/n/sklonnost-k-viktimnomu-povedeniyu-u-podrostkov-osobennosti-ego-proyavleniya (дата обращения: 23.09.2025).

11. Рыбакова Ольга Сергеевна. Безопасность несовершеннолетних в информационном обществе: анализ киберрисков и угроз // Мониторинг правоприменения. 2020. № 2(35). URL: https://cyberleninka.ru/article/n/bezopasnost-nesovershennoletnih-v-informatsionnom-obschestve-analiz-kiberriskov-i-ugroz (дата обращения: 23.09.2025).

12. В России в 2024 году IT-преступления достигли пика за последние пять лет // habr.com [сайт]. URL: https://habr.com/ru/news/877022/ (дата обращения: 23.09.2025).

13. В МВД назвали число преступлений против детей в 2024 году // ria.ru [сайт]. URL: https://ria.ru/20250919/rossija-2042868924.html (дата обращения: 05.09.2025).

14. Дети все чаще становятся жертвами киберпреступников // evening-kazan.ru [сайт]. URL: https://www.evening-kazan.ru/obshhestvo/news/deti-vsyo-chashche-stanovyatsya-zhertvami-kiberprestupnikov?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 10.09.2025).

15. Каникулы не для всех: аналитики фиксируют рост мошенничества в отношении школьников // forbes.ru [сайт]. URL: https://www.forbes.ru/novosti-kompaniy/538627-kanikuly-ne-dla-vseh-analitiki-fiksiruut-rost-mosennicestva-v-otnosenii-skol-nikov (дата обращения: 02.09.2025).

16. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // мвд.рф [сайт]. URL: https://мвд.рф/reports/item/60248328/(дата обращения: 02.09.2025).

17. С четырех лет – в интернет [Электронный ресурс] // rbc.ru [сайт]. URL: https://www.rbc.ru/newspaper/2025/03/03/67c1b67a9a7947a146b068c3 (дата обращения: 05.09.2025).

УДК 341

А. А. Смольяков,
кандидат юридических наук, профессор,
Заслуженный юрист Российской Федерации,
Ленинградский областной филиал
Санкт-Петербургского университета МВД России,
О. В. Гаврилова,
кандидат юридических наук,
старший преподаватель,
Ленинградский областной филиал
Санкт-Петербургского университета МВД России

К вопросу о методах борьбы с технологиями «дипфейк» в кибербезопасности

Аннотация. Рассматриваемые в рамках статьи технологии «дипфейк» в настоящий момент – реальная опасность кибербезопасности государства. В статье анализируются определенные способы противодействия рассматриваемых технологий, такие как алгоритмические, организационные и правовые меры. Рассмотрены достоинства и недостатки каждого из методов. Особое внимание уделено возможностям и перспективам развития каждого из них. Подчеркнута насущность целостного подхода и важность международного сотрудничества в данной сфере для плодотворного противостояния вреду, приносимому дипфейками.

Ключевые слова: технологии, кибербезопасность, «дипфейк», международное сотрудничество, правовое регулирование

A. A. Smolyakov,
Candidate of Law, Professor,
Honored Lawyer of the Russian Federation,
Leningrad Regional Branch of the
St. Petersburg University of the Ministry of Internal Affairs of Russia,
O. V. Gavrilova,
Candidate of Law,
Senior Lecturer,
Leningrad Regional Branch of the
St. Petersburg University of the Ministry of Internal Affairs of Russia

On the question of methods of countering "deepfake" technologies in cybersecurity

Abstract. The "deepfake" technologies discussed in this article currently pose a real threat to state cybersecurity. This article analyzes specific methods for countering these technologies, such as algorithmic, organizational, and legal measures. The

advantages and disadvantages of each method are discussed, with particular attention paid to the potential and development prospects for each. The urgency of a holistic approach and the importance of international cooperation in this area to effectively combat the harm caused by deepfakes are emphasized.

Keywords: technology, cybersecurity, deepfake, international cooperation, legal regulation

Введение. В настоящее время все большее распространение и активное внедрение получают различные кибертехнологии. Одними из таких технологий являются технологии «дипфейк», которые позволяют пользователям моделировать вполне действительные «картинки», которые, однако, являются подделкой. Современные разновидности возможностей аудио- и видео записывающих систем стали отличаться все большим совершенством и доступностью. В этой связи нельзя не отметить факт того, что это ведет к возникновению новых проблем, которые выражаются в опасности в сфере кибербезопасности: все более распространяющаяся дезинформация, усиливается процессы, связанные с манипуляциями общественным сознанием, не исключены также такие преступные деяния, как мошенничество и шантаж. Для устранения таких негативных последствий необходимо разрабатывать и внедрять эффективные способы для того, чтобы эффективно их обнаружить и противодействовать. Нельзя в стороне оставить и проблему, касающуюся спорных вопросов в правовом поле при решении вопросов, связанных с дипфецками. Немаловажно также в этой связи и повышение компьютерной грамотности граждан. Проблема технологий, связанных с искусственным интеллектом, вызывает неподдельный интерес у многих авторов, некоторые из которых убеждены, что в качестве инструмента информационных операций могут использоваться и дипфеки [4. С. 92-101].

Основная часть. Разработка последовательности машинного обучения, которые могут различать фейковый продукт от настоящего, является главным инструментом в борьбе с рассматриваемыми угрозами. Рассматриваемыми алгоритмами повергаются анализу различные признаки, связанные с не реалистичностью изображения, созданного с помощью искусственного интеллекта. Как пример, можно привести исследование в ходе которого был создан метод обнаружения дипфейков (подход, в основу которого был положен анализ частоты морганий). Исследователями из Калифорнии было установлено, что в действительности такой защитный рефлекс, как моргание глаз у людей происходит чаще, нежели в подделках видеоизображений. Это – один из важных показателей дипфейка.

Другими исследователями предлагаются подходы к обнаружению изображений-подделок на основе анализа статистических характеристик шума [2].

Еще один метод предлагает применять генеративно-состязательные сети для создания «меток» или «водяных знаков», которые при их создании могут быть встроены в конечный результат. Такие «знаки» помогают определить происхождение и подлинность, материала, выявить обнаруживать его видоизменения. Но, несмотря на все предосторожности, противоправными элементами могут быть предприняты различные приемы и методы, касающиеся возможностей

по удалению или подделки таких отметок. Все это приводит к необходимости к регулярной модернизации способов защиты. Техника встраивания робастных водяных знаков в видеопоток, устойчивых к всевозможным видам нападений была представлена А.А. Коробовым и М.Н. Фаворской [3].

Формирование способов установления дипфейков – нахождения автора и места производства противоправного интернет-контента является важным направлением хода современной научной мысли. Установление авторства и происхождения дипфейка окажет неоценимую помощь в выяснении и установлении обстоятельств противоправного деяния, расследовании преступного деяния, и привлечения виновных к самому суровому виду юридической ответственности – уголовной.

В рамках нашей статьи мы не могли не отметить и тот факт, что голландские ученые, проанализировав особенности работы генеративных моделей (StyleGAN) разработали способ определения дипфейков. Исследователями из Нидерландов было продемонстрировано, что различные образцы оставляют свойственные только им отпечатки в созданных «картинках», которые можно использовать для распознавания.

Свое видение проблемы было представлено и российскими исследователями, которыми была предложена идея идентификации генеративных моделей, основываясь на исследовании объектов в частотной области [6].

Вне всякого сомнения, в настоящее разработка различных средств обнаружения дипфеков развивается достаточно успешно и динамично, однако в этой сфере присутствуют некоторые ограничения:

– «творцы» дипфейков активно применяют новейшие достижения технической мысли и разрабатывают методы, преодоления существующих способов их обнаружения. Это обстоятельство способствует «обострению отношений» между учеными и представителями противоправного элемента и вызывает потребность в постоянном совершенствовании методов и способов.

– для проведения проверки образцов обнаружения и выявления необходимы значительные базы данных, включающих в себя как реальные, так и фальшивые изображения и видеоматериалы. Задача эта весьма трудна, энерго- и материально затратна. Кроме того, никто не исключает мнения экспертов в этой области, а также соблюдения норм этики и морали. Некоторыми авторами (Б.С. Ахметов и др.) активно рассматривается проблема создания и использования информационного массива, базы данных для выявления дипфейков, а также этическая и правовая стороны вопроса [1].

Особую, не менее значимую роль в противостоянии с дипфейками занимают организационные и правовые меры. Повышение компьютерной грамотности населения, информированность граждан по вопросам конкатенации в это играют одну из главных ролей. В связи с этим считаем необходимым просвещение граждан в области критического мышления, объективный подход и контроль источников информации, а также определение возможностей манипулирования сознания.

Главные и самые активные пользователи Интернета и цифровой информации – граждане молодого поколения. Поэтому актуальной проблемой являет-

ся совершенствование навыков цифровой грамотности именно у этой части населения. Нельзя не согласиться с мнением Г.У. Солдатовой, которая проблему, связанную с образованием молодежи в области приобретении навыков безопасности и ответственности поведения в цифровой среде, ставит в ряду важнейших в современном образовании детей и подростков [7].

В рамках нашей статьи мы не могли не затронуть и такого ответственного момента, касающегося вопросов формирования этических стандартов и норм поведения тех, кто занимается разработкой и внедрением материалов и информации.

На определенных медиаплатформах (Twitter, Reddit) и в социальных сетях в настоящее время наложен запрет на размещение «дипфейков», которые занимаются дезинформацией и манипулированием. Но отметим, что эти методы не всегда имеют должный успех.

Вестерлунд М. замечает, что представители противоправного элемента, с целью «заметания» и запутывания следов переходят на другие платформы или применяют зашифрованные каналы связи.

Использовать принципы ответственного поведения производителей и пользователей новейших технологий в цифровой сфере предлагает в своем исследовании Ю.М. Шаев [8].

Что касается ответственности за данные противоправные деяния, подчеркнем, что в США, КНР и др. были приняты нормативные правовые акты, направленные на борьбу с «дипфейками» и защиту, в связи с этим прав граждан. За совершение подобных правонарушений и преступлений предусматривается юридическая ответственность.

Но, по мнению некоторых авторов (Чесни Р.), в настоящее время нормами права не всегда учитывается специфика дипфейков, и принятые, в связи с этим явлением нормативные правовые акты требуют серьезной доработки [9].

Отечественные исследователи, в том числе А.А. Ефремов, не обошли своим вниманием правовые вопросы, касающиеся применения дипфейков, и решением этих проблем в области права. Нашими соотечественниками тщательно анализируется лучший зарубежный опыт в этой области и на его основании выбираются оптимальные варианты решения спорных вопросов [3].

В этой связи нельзя обойти вниманием и проблему правового регулирования в области защиты прав на свободу слова и творческого выражения.

Некоторые правоведы выражают свое опасение, что чрезмерное упорядочение в данной сфере может вылиться в ограничении законных форм использования технологий дипфейк. К решению этой проблемы нужно подходить очень вдумчиво и осторожно. Авторы статьи убеждены в необходимости баланса между защитой от вредоносных проявлений цифровых достижений и сохранением интернет-ресурсов для творчества и самовыражения.

Активное развитие новейших цифровых технологий, влечет за собой вместе с позитивными моментами и появление новых (явных и скрытых) угроз. Методы противостояния новым опасностям должны постоянно расширяться, оттачиваться, обогащаться.

Формирование новых способов обнаружения дипфейков в реальном времени, которые могли бы автоматически «рассматривать» информацию, как сразу она появилась – одно из многообещающих направлений, что повлечет за собой совершенствование последовательности работы на мобильных устройствах и консолидации с платформами социальных сетей и мессенджеров.

Формирование децентрализованных систем верификации информации на основе технологий «Блокчейн» стало важным направлением. Такие структуры могли бы позволять оставаться информации об авторе и происхождении информации неизменной и «прозрачной», и вместе с тем также побуждать и поощрять пользователей к правомерному поведению в Сети. Нельзя сбрасывать со счетов и репутационные составляющие процесса, а также возможную систему поощрений.

Принимая во внимание планетарный характер проблемы, нельзя не обойти вниманием и международное сотрудничество в данной сфере. Международное сотрудничество в рассматриваемом нами контексте является одной из важнейших граней в борьбе с «дипфейками». Вне всякого сомнения, назрела насущная потребность в разработке международных норм и правил обмена информацией о «дипфейках», а также консолидация труда сотрудников правоохранительных органов и общественных организаций всех государств мира.

Заключение. Только объединив все силы и мощь государств мира, возможно противостоять все большим возникающим опасностям в цифровом мире, гарантировать защищенность, сохранность и подлинность информации.

Рассматриваемые нами в рамках нашей статьи технологии в настоящий момент – реальная угроза кибербезопасности государства, которая предполагает всесторонний подход и постоянной рационализации, и модернизации.

Список литературы

1. Ахметов Б.С., Тасмагамбетов И.Н., Мухамбеткалиев Е.Е. Анализ методов выявления поддельных изображений и видео, сгенерированных с помощью нейронных сетей // Вестник Национальной академии наук Республики Казахстан. 2021. № 2. С. 51-58.

2. Гаврилов А.И., Сидоров К.В., Окунев А.В. Метод обнаружения поддельных изображений на основе анализа шумовых характеристик // Компьютерная оптика. 2021. Т. 45. № 2. С. 239-248.

3. Ефремов А.А. Правовое регулирование технологии «дипфейк»: зарубежный опыт и российская перспектива // Вестник Санкт-Петербургского университета.

4. Красовская Н.Р. Технологии искусственного интеллекта как инструмент информационных операций // Международная жизнь. 2020. № 6. С. 92-101.

5. Коробов А.А., Фаворская М.Н. Метод встраивания цифровых водяных знаков в видеопоток на основе трехмерного вейвлет-преобразования // Информационно-управляющие системы. 2020. № 6. С. 74-82.

6. Мурашов Д.М., Коробов А.А., Фаворская М.Н. Идентификация генеративных состязательных сетей на основе анализа частотных характеристик изображений // Компьютерная оптика. 2022. Т. 46. № 2. С. 296-306.

7. Солдатова Г.У., Рассказова Е.И., Чигарькова С.В. Цифровая компетентность российских подростков и родителей: результаты всероссийского исследования // Национальный психологический журнал. 2020. № 2 (38). С. 3-14.

8. Шаев Ю.М. «Дипфейки как этическая проблема // Гуманитарные и социально-экономические науки. 2021. № 3 (118). С. 33-37.

9. Chesney R., Citron D.K. Deep Fakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics // Foreign Affairs. 2019. Vol. 98. № 1. P. 147-155.

УДК 343

А. Д. Цыплакова,
преподаватель,
Московский государственный институт
международных отношений
Министерства иностранных дел
Российской Федерации

Игры как криминогенный фактор и мера виктимологической профилактики киберпреступлений

Аннотация. В настоящей работе кибердеяния рассматриваются как любое использование информационно-коммуникационных технологий в преступных целях. С криминологической точки зрения игры можно рассматривать как криминогенный фактор множества различных преступлений: насильственных (проявление агрессии в разной степени), корыстных (деяния против собственности по типу кражи и разбои, отмывание активов, полученных преступным путем, финансирование терроризма, экстремизма и запрещенных организаций, дропперство), компьютерных (иные виды дропперства) и против общественной безопасности (распространение опасных идеологий и вредоносного контента). Противодействие подобной криминогенной ситуации должно носить комплексный характер: начиная от искоренения причин и условий, личностного формирования и заканчивая привлечением к уголовной ответственности (при надлежащей криминализации и пенализации). Формирование так называемого цифрового иммунитета лица должно обеспечиваться на всех стадиях совершения административно и уголовно наказуемых правонарушениях. При этом и сами игры могут рассматриваться как одна из мер виктимологической профилактики традиционных и киберпреступлений с раскрытием сценариев жертв и преступников, а также должны иметь ряд ограничений, соответствующих существующим и формирующимся международным стандартам, в том числе международного гуманитарного права и проблемного контента.

Ключевые слова: киберпространство, игровая индустрия, киберпреступления, профилактика преступлений, виктимология, цифровой иммунитет, кибероосведомленность, цифровая грамотность

A. D. Tsyplakova,
PhD candidate, Lecturer,
MGIMO University

Games as a crime-generating factor and a cybercrime victimological preventive measure

Abstract. The author of the article defines cybercrime as any use of information and communication technologies for criminal purposes. From a criminological point of view, games can be considered a criminogenic factor in a variety of

crimes: violent (aggression), mercenary (acts against property such as theft and robbery, money laundering, financing of terrorism, extremism and prohibited organizations, mules), computer crimes (other types of so-called droppers) and crimes against public safety (the spread of dangerous ideologies and harmful content). Countering such a crime-prone situation must be comprehensive in nature: starting with the eradication of causes and conditions, personal development and ending with criminal prosecution (inter alia appropriate criminalization and penalization). The formation of a person's so-called digital immunity must be ensured at all stages of committing administrative and criminal offences. Meanwhile, the games themselves can be seen as one of the ways to prevent traditional and cybercrimes by revealing the scenarios of victims and criminals, and should have a number of restrictions that meet existing and emerging international standards, including international humanitarian law and problematic content.

Keywords: cyber reality, game industry, cybercrimes, crime prevention, victimology, digital immune, cyber awareness, digital literacy

Введение. В России насчитывается более 25 миллионов геймеров, более половины населения (61 %) регулярно играет в видеоигры (около трети – ежедневно). С точки зрения портрета геймера характеристика разнится у аналитиков: как мужчина-миллениал с высшим образованием и средним доходом, состоящий в браке с детьми, так и более молодое поколение (зумеры) играют на мобильных устройствах [1–3]. При этом подростки в два раза чаще становятся жертвами киберпреступлений, а игры доходят до патологического влечения и зависимости [4, 5. С. 139].

Основная часть. В законодательстве Российской Федерации не содержится понятийного аппарата в игровой индустрии (также именуемой гейминг от англ. "gaming"), за исключением «компьютерного спорта», который был внесен во Всероссийский реестр видов спорта в 2001 году, исключен и повторно добавлен в 2016 году на основании соответствующего приказа Министерства спорта Российской Федерации № 470 от 29 апреля 2016 г. [6]. Тем не менее рассматриваемая индустрия не ограничивается компьютерным спортом (часто в литературе именуемый киберспортом) и требует более детального изучения.

Игровая индустрия как развлекательный способ времяпровождения многих пользователей может служить как источником криминогенной ситуации для совершения традиционных и киберпреступлений, так и мерой виктимологической профилактики. В то время как с первым могут возникать проблемы на этапе квалификации деяний и не защищенных законом отдельных благ, второе требует грамотного подхода.

Что касается типичных посягательств, связанных с игровой индустрией, *во-первых*, агрессивные типы более склонны к совершению преступлений против личности. При злоупотреблении насильственными играми прайминг выражается в фиксации специфический воспоминаний, которые лица, особенно несовершеннолетние, могут впоследствии воспроизводить в реальности и сохранять чувство, что находятся все еще в игре, которая сформировала преступный стереотип поведения [7. С. 58]. Подобное может быть причиной не только

насильственных, но и насильственно-корыстных деяний, ведь денежные средства на приобретение улучшений, совершенствование навыков и лидерство в игре также могут выступать в качестве мотива преступлений против собственности (краж, грабежей и разбоев) [8. С. 363]. Очевидно, что в поисках заработка возможно применение опыта из игр и использование преступных способов для более быстрого достижения результата, тем самым создавая порочный круг.

В случае с злоупотреблениями и зависимостью, помимо родительского контроля, возможно ограничение игрового времени при обязательной авторизации в аккаунтах, подконтрольных или связанных с государством. Так, например, В сентябре 2020 года в Китайской Народной Республике была введена обязательная идентификация игроков с помощью единой государственной системы (аналог в Российской Федерации – Единый портал государственных услуг). Вдобавок, некоторые виды игр (e.g., лутбоксы) имеют двойственную природу и могут быть охарактеризованы как азартные (по игровому движку или согласно регулированию конкретной страны).

Во-вторых, виртуальные объекты могут одним из элементов схем отмывания активов, полученных преступным путем, финансирования запрещенных организаций, терроризма и экстремизма (ОД/ФТ), в особенности через сторонние сервисы по обмену и торговле игровыми предметами, а также краудфандинг. В то время как официальные игровые платформы по типу «Steam» не допускают вывода денежных средств, существует множество так называемых сервисов-зеркал и аукционных площадок, которые позволяют игрокам в обход официальных это делать [9]. Несмотря на заявления по следованию принципам KYC (с англ. «know your client» – «знай своего клиента»), отметим, что с развитием нейронных сетей полагаться на изображение как доказательство и способ идентификации лица может стать опрометчивым решением. Использование "ChatGPT-4o" технологическим предпринимателем и венчурным инвестором Борисом Муселяком для фальсификации паспорта в качестве эксперимента доказывает это [10]. Отсутствие единых методик и инструментария для выявления сгенерированного искусственным интеллектом контента при проведении экспертиз, да и достаточного количества квалифицированных специалистов лишь осложняют выявление преступной деятельности. В то время как крупные компании по типу "OpenAI", "Meta"[1], "Google", "Tiktok", "Youtube", "X" внедряют различные виды маркировок, в том числе водяные знаки, множество стартапов и более мелких сервисов не всегда могут следить за подобным ввиду отсутствия национальных законодательных требований (не говоря уже о международных стандартах). Интересен в этой связи китайский опыт – Меры по генерации искусственного интеллекта и идентификации синтетического контента от 7 марта 2025 г. [11] обязывают внедрять как явную, так и неявную маркировку сгенерированного контента в метаданных и самих электронных файлах.

[1] Организация признана экстремистской на основании решения Тверского районного суда Москвы от 21 марта 2022 г.

Схемы ОД/ФТ могут быть не только непосредственно с внутриигровыми объектами, но и аккаунтами, в том числе Apple ID / Google Play. Оплата может производиться незащищенными методами и служить элементом схемы ОД/ФТ с мобильных приложений по типу "Clash of Clans", "Clash Royale" и "Marvel Contest of Champions". Сначала имеет места кража данных банковских карт мошенниками, далее производится их привязка к идентификаторам в магазинах приложений по типу "SuperCell ID", а также скупка игровых предметов с последующей продажей аккаунтов через сервисы по типу "g2g.com" [12]. Сложности заключаются в неопределенности правовых статусов отдельных цифровых объектов, в том числе виртуальных активов и внутриигровых предметов, которые лишь частично признаются предметом преступления. Исходя из положения Постановления Пленума Верховного Суда Российской Федерации № 32 от 7 июля 2015 г. «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» (в ред. от 26 февраля 2019 г.) указывается, что предметом ОД могут быть «*денежные средства, преобразованные из виртуальных активов (криптовалюты)*» [13]. В то время как банковские реквизиты в подобных схемах могут расцениваться как персональные данные и посягательства на них запрещены уголовным законом, то оценить экономическую ценность так называемого виртуального имущества представляется сложным (а иногда и невозможным) при квалификации, например, хищений. Вдобавок, в отличие от кредитных учреждений, которые активно сотрудничают с правоохранительными органами, игровые платформы, находясь на недружественных юрисдикциях, могут отказывать в подобном.

При этом распространена практика так называемого *дропперства*, которая не ограничивается SIM-картами или абонентскими номерами, но включает в себя сдачу всевозможных аккаунтов в аренду как на постоянной коммерческой (профессиональной), так и на разовой основах при поиске так называемого легкого заработка. В июле 2025 г. были последовательно приняты законопроекты об уголовной ответственности за деятельность нескольких видов дропов: в сфере электронных средств платежа (ст. 187 УК РФ [14]), SIM-бокса или виртуальной телефонной станции (ст. 274.3 УК РФ), абонентских номеров (ст. 274.4 УК РФ), информации для регистрации и/или авторизации для получения доступа к Интернет-ресурсам (ст. 274.5 УК РФ [15]). Отметим специфичность построения норм как одно из возможных препятствий для эффективного привлечения лиц к ответственности как одного из направлений противодействия киберпреступности:

– организация деятельности как основа объективной стороны встречается в ст. 205.5 и ст. 282.2 УК РФ, охватывая действия организационного характера, направление на возобновление или продолжение противоправной деятельности конкретной *организации*, исходя из положений Постановления Пленума Верховного Суда Российской Федерации № 1 от 9 февраля 2012 г. «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» (в ред. от 3 ноября 2016 г.) [16]; организация деятельности как основа объективной стороны в ст. 110.2 УК РФ не имеет разъяснений в

рамках ППВС РФ, однако имеет обширную судебную практику и обычно сводится к ведению аккаунтов в социальных сетях (каналов в мессенджерах) и созданию закрытых бесед (чатов) с призывами к самоубийству или инструкциями по его совершению; следовательно, организация деятельности по передаче абонентских номеров и сведений для авторизации/регистрации на Интернет-ресурсах фактически охватывает действия организатора (как одной из форм соучастия);

– участие в деятельности (ст. ст. 205.5, 282.2 и 284.1 УК РФ) подразумевает продолжение или возобновление деятельности *организации*, распространение материалов, участие в мероприятиях *организации* и их организация, предоставление помещений для их проведения, однако в случае со ст. 274.4 и ст. 274.5 УК РФ о непосредственных исполнителях – те, кто получает информацию для совершения иного преступления, а также *вероятно* те, кто предоставляет информацию для авторизации и/или регистрации за вознаграждение.

Возникает вопрос: передача информации для авторизации и прокачки аккаунта в играх третьим лицам за вознаграждение может ли попадать под действие ст. 274.5 УК РФ, ведь элементы субъективной стороны имеют альтернативный характер: корыстная заинтересованность или совершение иного преступления. Учитывая п. 16 Постановления Пленума Верховного Суда Российской Федерации № 19 от 16 октября 2009 г. «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» (в ред. от 11 июня 2020 г.) [17], корыстная заинтересованность подразумевает стремление получить выгоду для себя или третьих лиц имущественного характера посредством совершения *неправомерных* действий. В зарубежных странах (e.g., в Южной Кореи с 2018 г.) «прокачка» (англ. «boosting») и перепродажа аккаунтов в играх являются уголовно наказуемыми. Превентивной целью рассматриваемой нормы, конечно, является в первую очередь пресечение аренды аккаунтов в социальных сетях и мессенджерах для мошеннических целей, кражи персональных данных и последующего шантажа, взлома связанных аккаунтов (эффект Домино), цифрового вандализма, рассылок фишинговых ссылок, вредоносного программного обеспечения, спама, кражи личности, вербовки, распространения запрещенного контента или финансовых махинаций. Тем не менее в случае, если игровой аккаунт будет фактически использоваться для обеления денежных средств под видом прокачки или улучшения персонажей, то подобные действия будут образовывать состав преступления.

В-третьих, онлайн-игры можно рассматривать в качестве способа общения и передачи информации, что в свою очередь превращает их в пространство для негативного влияния на личность, пропаганды идей, противоречащих законодательству государства, распространения запрещенных идеологий (терроризма и экстремизма). Сложность заключается в выявлении подобных платформ и различиях в понимании проблемного контента, который не охватывается ни одной из существующих конвенций универсального или регионального уровней.

Что касается комплекса мер противодействия преступности в игорной деятельности, то они должны быть направлены на личностное формирование и изменение обстоятельств. На доинцидентном уровне через модель безопасности индивидуума (в целом) и безопасное использование гаджетов и игровой деятельности (как частный случай) возможно формирование нейтрально-позитивного поведения [18, 19]. Лицо должно перестать представлять подходящую цель для преступника, тем самым исключая один из элементов теории рутинных действий Фэлсона и Коэна [20. С. 392].

Рис. 1. Теория рутинных действий

Одним из примеров просветительских интерактивных проектов для снижения виктимности и лучшего понимания природы правонарушений в киберпространстве могут быть и сами онлайн-игры, особенно в части противоправного контента. В «Кошмаре модератора» (англ. "Moderator Mayhem") игрок выступает в качестве модератора пользовательского контента на вымышленной социальной платформе "Trust Hiver" с точки зрения дискриминации, спама, угроз, насилия, нарушения законодательства, политических дискуссий и с получением комментариев менеджера, мнения общественности и возможным повторным рассмотрением в случае ошибки на основании раздела 230 Закона США от 19.06.1934 «О коммуникациях» [21, 22]. В последующих раундах рассматриваются апелляции или комментируются советы ИИ-помощника. Кошмар модератора был разработан компанией "Engine", Рэнди Любином и Майком Масником (блогерами "Techdirt").

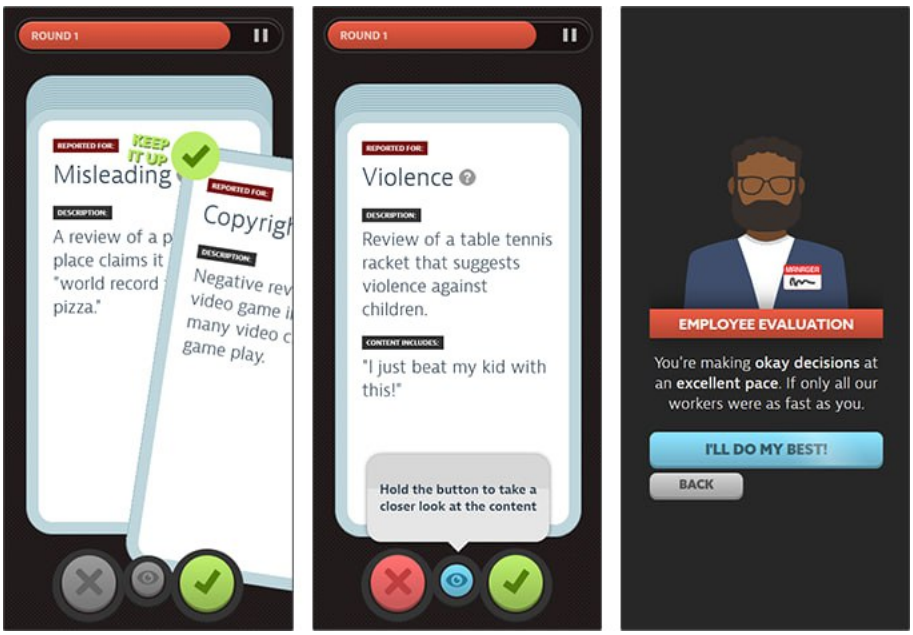


Рис. 2. Игра «Кошмар модератора»

Позднее было разработано продолжение – «Магнат доверия и безопасности» (англ. "Trust & Safety Tycoon") по развитию политике конфиденциальности социальной платформы "Yapper", найму модераторов и их руководству и автоматизации отдельных процессов [23]. Разработчики основывались на опросах соответствующих служб в компаниях и приблизили к политическим и техническим дилеммам, с которыми сталкиваются сети и мессенджеры, а также законодательные требования: передача данных по запросу правоохранительных органов, фишинг, кибератаки, противоправный и проблемный контент, преступление как услуга, спорные ситуации и резонансные информационные поводы.

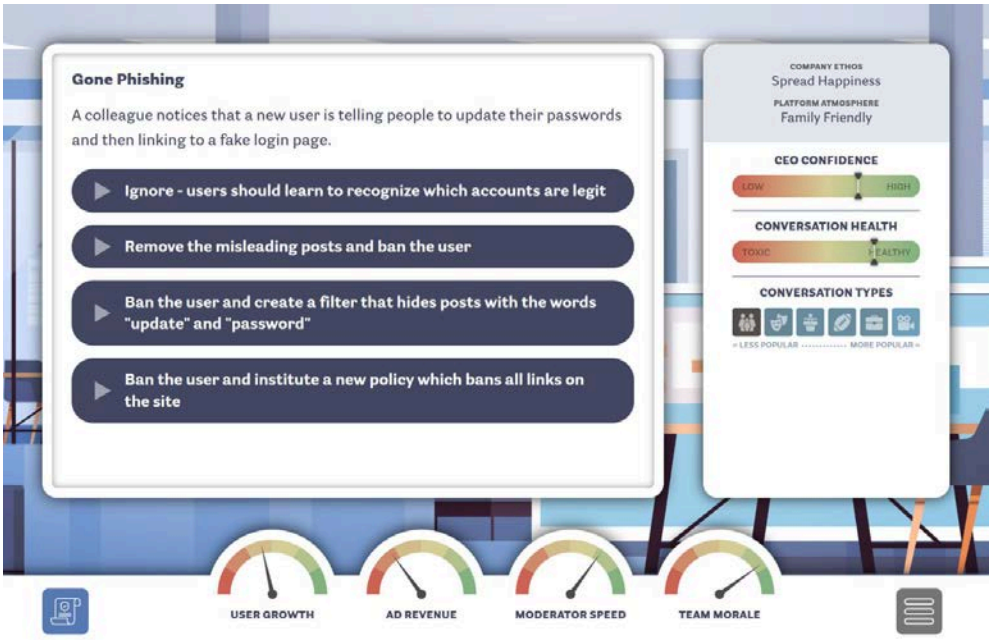


Рис. 3. Игра «Магнат доверия и безопасности»

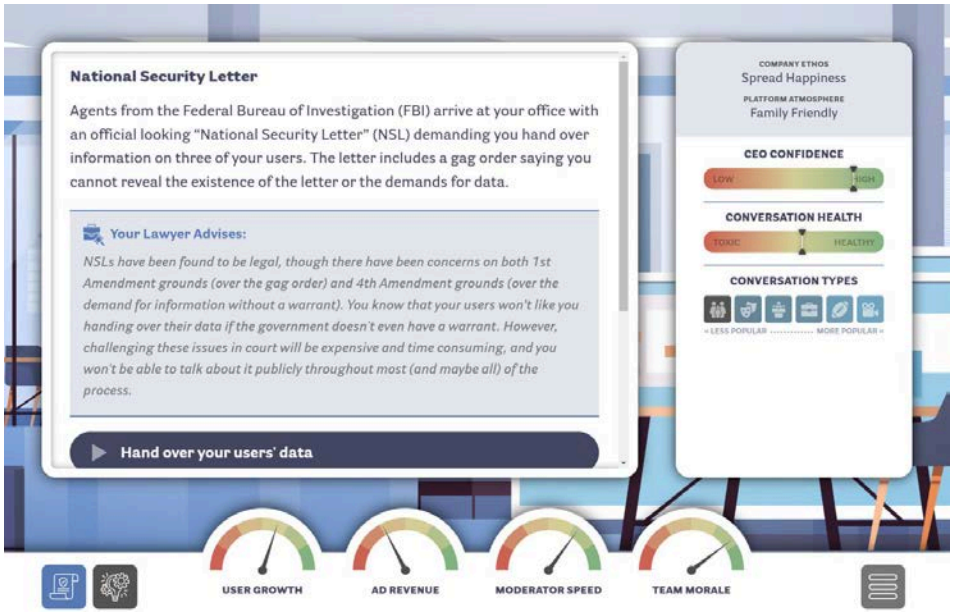


Рис. 4. Игра «Магнат доверия и безопасности»

Недавно разработчики ("Techdirt") совместно с Международным комитетом Красного Креста (МККК) выпустили дополнение «Доверие и безопасность. Вооруженный конфликт» (англ. "Trust & Safety. Armed Conflict"), где меняются обстоятельства: боевые действия между вымышленными странами (Альпесией и Сольферинией) на основании реальных событий и затрагивают защиту данных, недостоверные объявления, жестокие видеозаписи, передачу сведений государственных органов, проведение экспертиз, торговлю людьми, контрабанду мигрантов с интерактивными ссылками на описание международных стандартов в области прав человека и международного гуманитарного права, просветительские видеоролики и веб-сайты. Перечисленные три игры похожи на «Документы, пожалуйста!» (англ. "papers, please! "), однако содержат нормы законодательства реального существующего государства (США) и международного права.

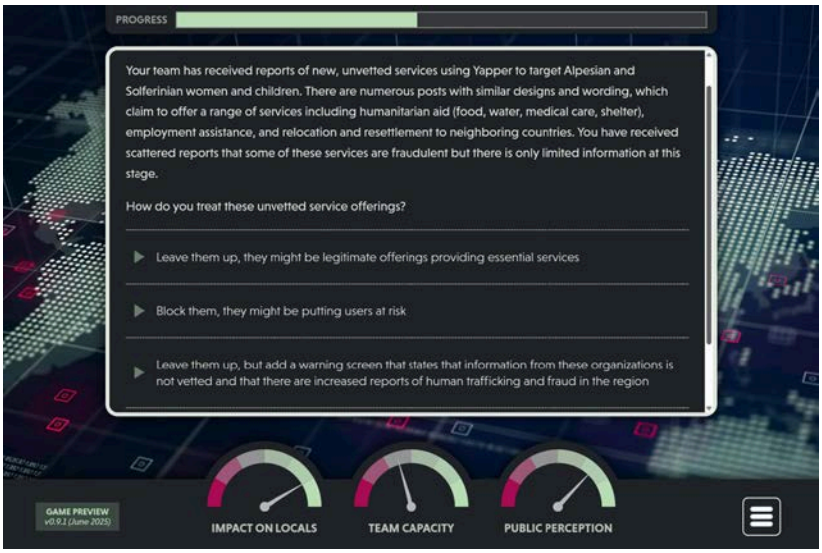


Рис. 5. Игра «Доверие и безопасность. Вооруженный конфликт»

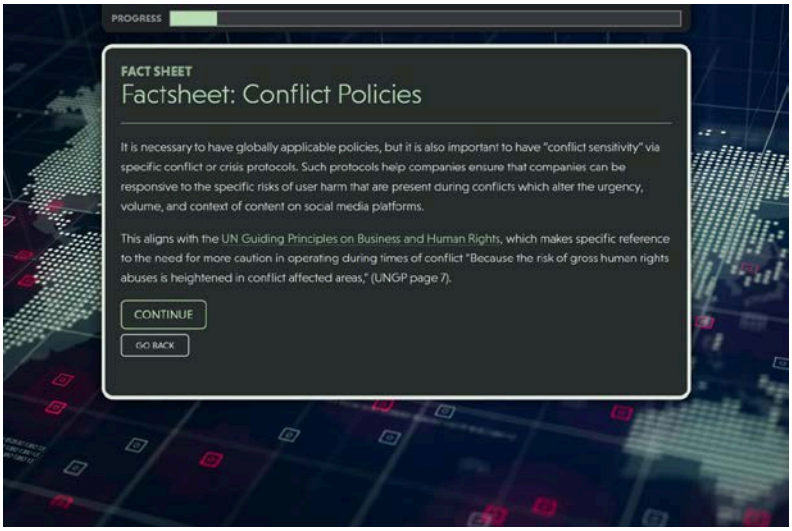


Рис. 6. Игра «Доверие и безопасность. Вооруженный конфликт»

Вдобавок, хотя игры основываются на реальных исторических событиях и содержат указания на вымысел, заимствования могут восприниматься буквально, тем самым искажая представление о действительности. Используемая система психологических манипуляций и абсолютная вседозволенность формируют некорректные ценностные установки [24]. Излишняя жестокость и нарушение обычных норм международного гуманитарного права как стиль игры может негативно сказываться на «поля сражений в реальной жизни». По этой причине Международный комитет Красного Креста издал заявление с указанием на необходимость соблюдения «настоящих правил войны» в виртуальной реальности: не добивать поверженных врагов, не стрелять по безоружным неигровым персонажам (англ. "NPCS"), не атаковать гражданские объекты, делиться аптечкой со всеми раненными. В подобной акции участвовали стримеры, а также внедрены специальные режимы в играх "Arma 3" и "Fortnite" [25]. Тем не менее боевые действия ряда шутеров изначально ведутся на территории гражданской инфраструктуры («PUBG Battlegrounds»), в них нельзя поделиться аптечкой ("Counter-Strike"), что осложняет расширение подобной кампании. В 2017 г. была также выпущена онлайн-игра «Не будь онемевшим» (англ. "Don’t be Numb") на английском, французском и испанском языками с квизом и визуализацией норм МГП (Женевских конвенций) [26].

Еще одними примерами могут быть игра в классики (англ. "Rayuela game"), разработанная в рамках проекта, финансируемого за счет грантовой программы Европейского Союза «Горизонт 2020» с шестью приключениями на тематики: кибербуллинг, фишинг, онлайн-груминг и фэйковые новости [27], а также игра «Лаборатория кибербезопасности» (англ. "Cybersecurity Lab") игрок – сотрудник социальной платформы "Einstagram", "SnapCat", "WattsAmp" или "Phasebook" – должен следить за кибербезопасностью и отбивать кибератаки. Подобные стартапы реализуются в значительной мере в США и Европе [28, 29].

Другим направлением профилактических мер служит встраивание в уже существующие игры элементы противодействия. Так, в рамках платформы «Roblox» Европол создал игру «Кибер Защитники» (англ. "Cyber Defenders") для поимки киберпреступников и объяснения отдельных их схем: кражи личности, мошенничество и груминг [30].

Более осознанный подход позволил бы закладывать конкретные ценности, соответствующие международным стандартам, в игровых формах, однако подобных проектов немного и касаются либо киберпреступлений, либо военных преступлений. С одной стороны, это связано с тем, что самым популярным жанром являются ролевые и приключенческие экшен и шутеры, с другой – именно они потенциально могут повышать криминогенность. Отдельные явления по типу читерство[2] в (на первый взгляд) безобидных симуляторах могут быть условием формирования преступного поведения, исходя из теории рутинных действий: чувство превосходства, любопытства, отсутствие анти-читерских политик или легкодоступность их обхода / отключения, невосприятие оппонентов и игроков как живых лиц, а объектов приводит к определенному паттерну [31].

Развитие так называемого цифрового иммунитета могло бы опираться не только чисто на просветительские проекты, в рамках которых в доступной форме рассказывают правила кибергигиены и повышают осведомленность и проверяют цифровую и финансовую грамотность, но и на изменение условий – модель окружающей среды, ведь виртуальное пространство становится неотъемлемой частью жизни. Нераспространение правил либо пробелы в существующем регулировании требуют коренных изменений – длительный процесс, который может начаться с более мелких и простых шагов: внедрение соответствующих практик в игровой процесс и развитие кластера игр, прививающих кибервоспитание и повышающих киберосведомленность. Причем подобная практика может касаться противодействия не только киберпреступлений, но и иных видов деяний.

Игровой метод обучения эффективен не только в отношении несовершеннолетних [32], но и взрослых [33]. Симуляция сценариев-жертв помогает понять уязвимости с минимальными затратами, сценариев-преступников – схемы по вовлечению в преступную деятельность, что соответствует дидактическим основам виктимологии [34]. Они могут быть в виде квизов, головоломок, стратегий и ролевых, а также фокусироваться на технических или человеческих аспектах. При этом исследования показывают, что фокус скорее смещен на первые [35, 36]. Важно, чтобы игры достаточно достоверно отражали реальность для адекватной оценки рисков и угроз со стороны киберпространства. Примером служит многоступенчатая и многоуровневая игра «Киберпреступность»

[2] Обман, использование кодов и практик для нечестной быстрой прокачки аккаунта и персонажей.

(англ. «Cyber Crime Game») – обучение понимания мышления хакеров на примере собирательного образа-фантома (англ. «PhantomX») [37].

Заключение. Таким образом, игры могут служить как во благо, так и прямым или опосредованным инструментом преступников с точки зрения традиционных (экономических и против общественной безопасности) и кибердеяний. Риски заключаются в злоупотреблении играми, чрезмерном насилии, размытии границ между реальностью и виртуальностью, читерстве (как следствие, чувства вседозволенности), недостоверности фактов, отсутствии правового статуса отдельных элементов и целых видов игр, а также пробелов в регулировании игровой индустрии в целом и криминализации отдельных преступных схем в частности. Исходя из теории рутинных действий и отдельных направлений виктимологической профилактики, отметим важность формирования правильных ценностей и установок. В настоящей работе приведены примеры, которые могут служить ориентиром для развития отечественных разработок в игровой индустрии с целью снижения криминогенной обстановки. При этом важно помнить о превентивной, а не развлекательной цели.

Список литературы

1. Исследование Т-Банка: 61% россиян регулярно играют в компьютерные игры. 2025. Август. URL: https://www.tbank.ru/about/news/26082025-t-bank-research-61percent-of-russians-play-computer-games-regularly/ (дата обращения: 28.08.2025).

2. Тренды развития российского геймдева в 2025 году. 2024. Декабрь. URL: https://blog.rt.ru/b2c/trendy-razvitiya-rossiiskogo-geimdeva-v-2025-godu.htm (дата обращения: 28.08.2025).

3. Институт развития интернета. Компьютерные игры и метавселенные 2025. 2025. Март. URL: https://ict.moscow/analytics/kompiuternye-igry-i-metavselennye-2025/ (дата обращения: 28.08.2025).

4. Подростки в два раза чаще становятся жертвами киберпреступников – Сидоренко. 2024. Апрель. URL: https://rapsinews.ru/digital_law_news/20240418/309824212.html (дата обращения: 28.08.2025).

5. Каменская В.Г., Томанов Л.В. Цифровые технологии и их влияние на социальные и психологические характеристики детей и подростков // Экспериментальная психология. 2022. № 15(1). С. 139–159.

6. Приказ Министерства спорта России № 183 от 16.03.2017 «О признании и включении во Всероссийский реестр видов спорта спортивных дисциплин, видов спорта и внесении изменений во Всероссийский реестр видов спорта». URL: http://publication.pravo.gov.ru/Document/View/0001201704140005 (дата обращения 01.09.2025).

7. Лебедев И.Б., Филатова Т.П. Кибернетическая лудомания – новая область психологических исследований криминальной агрессии подростков // Психопедагогика в правоохранительных органах 2013. № 1 (52). С. 55-59.

8. Никитина Л.Н. Компьютерные игры с элементами насилия как источник посылов к агрессии у несовершеннолетних // Азимут научных исследований: педагогика и психология. 2018. Т. 7. № 3 (24). С. 361–364.

9. Цыплакова А. Д. Риски отмывания (легализации) активов, полученных преступным путем, и финансирования терроризма в сфере гейминга // Актуальные вопросы обеспечения национальной безопасности: материалы II Международной научно-практической конференции, Санкт-Петербург, 07 декабря 2023 года. Санкт-Петербург, 2024. С. 50–55.

10. Пару минут – и новый паспорт: ChatGPT обманул проверку личности. 2025. Апрель. URL: https://www.securitylab.ru/news/557958.php (дата обращения 01.09.2025).

11. 关于印发《人工智能生成合成内容标识办法》的通知 [Уведомление об издании Мер по созданию искусственного интеллекта и идентификации синтетического контента] // Управление киберпространства КНР. 14.03.2025. URL: https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm (accessed 23.08.2205).

12. Lishcuk R. 6 Major Data Breaches We Found and Reported in 2018. 2021. Июнь. URL: https://mackeeper.com/blog/data-breach-reports-2018/#. (дата обращения 01.09.2025).

13. О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем: Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_182365/ (дата обращения 01.09.2025).

14. О внесении изменений в статью 187 Уголовного кодекса Российской Федерации: Федеральный закон от 24.06.2025 № 176-ФЗ // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_508353/ (дата обращения 01.09.2025).

15. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2025 № 282-ФЗ // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_511071/ (дата обращения 01.09.2025).

16. О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности: Постановление Пленума Верховного Суда РФ от 09.02.2012 № 1 (ред. от 03.11.2016) // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_125957/ (дата обращения 01.09.2025).

17. О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий: Постановление Пленума Верховного Суда РФ от 16.10.2009 № 19 (ред. от 11.06.2020) // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_93013/ (дата обращения 01.09.2025).

18. Григорян В. К. Предупреждение преступности в высокоразвитых зарубежных странах // Актуальные проблемы российского права. 2012. № 4. С. 272–279.

19. Гришко Н.А. Защита потенциальных жертв киберпреступлений: виктимологический подход // Вестник Университета имени О.Е. Кутафина (МГЮА). 2025. № (5). С. 234–243.

20. Felson M., Cohen L.E. Human Ecology and Crime: A Routine Activity Approach // Human Ecology. 1980. № 8 (4). P. 392.

21. Protection for private blocking and screening of offensive material (47 U.S.C. § 230). URL: https://www.law.cornell.edu/uscode/text/47/230 (дата обращения 29.08.2025).

22. MODERATOR MAYHEM: A GAME TO TEST YOUR CONTENT MODERATION SKILLS. 2023. Май. URL: https://www.engine.is/news/category/moderator-mayhem (дата обращения 29.08.2025).

23. Trust & Safety Tycoon: Try Your Hand At Managing A Social Media Trust & Safety Team. 2023. Октябрь. URL: https://www.techdirt.com/2023/10/17/trust-safety-tycoon-try-your-hand-at-managing-a-social-media-trust-safety-team/ (дата обращения 01.09.2025).

24. Хавкин А.Б. Компьютерные игры как инструмент формирования образа врага. 2023. Июнь. URL: https://russiancouncil.ru/blogs/laiamp/kompyuternye-igry-kak-instrument-formirovaniya-obraza-vraga/ (дата обращения 01.09.2025).

25. Play by the rules. URL: https://playbytherules.icrc.org/ (дата обращения 01.09.2025).

26. Choosing humanity: new video and online game challenge us to confront how numb we have become to abuses to the rules of war. 2017. Ноябрь. URL: https://www.icrc.org/en/document/choosing-humanity-new-video-and-online-game-challenge-us-confront-how-numb-we-have-become-0 (дата обращения 01.09.2025).

27. RAYUELA game. URL: https://www.rayuela-h2020.eu/rayuela-game/?lang=en (дата обращения 01.09.2025).

28. Break Time! 8 Online Cybersecurity Games that You'll Love. 2023. Октябрь. URL: https://www.fortra.com/blog/8-online-cybersecurity-games-that-test-your-cyber-skills (дата обращения 01.09.2025).

29. Cybersecurity Games. Texas A&M University. URL: https://it.tamu.edu/security/cybersecurity-games/index.php (дата обращения 01.09.2025).

30. Cyber Defenders. Raising awareness for cybercrime via Roblox. 2024. Декабрь. URL: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/cyber-defenders (дата обращения 01.09.2025).

31. Cho S., Lusthaus J., Flechais I. The Slippery Slope: Exploring the Parallels Between Game Cheating and Cybercrime Through Routine Activity Theory. 2023 APWG Symposium on Electronic Crime Research (eCrime). 2023. Ноябрь. URL: https://www.researchgate.net/publication/379494626_The_Slippery_Slope_Exploring_the_Parallels_Between_Game_Cheating_and_Cybercrime_Through_Routine_Activity_Theory (дата обращения 01.09.2025).

32. Терешкевич О.В. Игра как активный метод обучения. Учительный журнал. 2025. Февраль. URL: https://www.teacherjournal.ru/categories/24/articles/10184 (дата обращения 01.09.2025).

33. Дубровская Е.С., Рожнева Е.М. Специфика игрового метода обучения взрослых в историческом дискурсе становления игровой деятельности как педагогического явления // Интерэкспо Гео-Сибирь. 2018. № 6. С. 148-151.

34. Жмуров Д.В. Общая виктимологическая профилактика киберпреступности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 135-142.

35. The Benefits of Cyber Security Games for Enhancing Online Protection. 2023. December. URL: https://www.institutedata.com/blog/benefits-of-cyber-security-games/ (дата обращения 01.09.2025).

36. Chiu Yeong Ng, Mohammad Khatim Bin Hasan. Cybersecurity serious games development: A systematic review. Computers & Security. 2025. № 150. 104307.

37. The Cyber Crime Game. URL: https://cybercrimegame.com/the-game/ (дата обращения 01.09.2025).

УДК 343.9

В. А. Шуняева
кандидат юридических наук, доцент
Тамбовский государственный университет
имени Г. Р. Державина

Психофизиологические особенности цифровых аддикций представителей цифрового поколения

Аннотация. Цель статьи, обозначить проблему цифровых аддикций представителей цифрового поколения, способствующих их криминализации. Цифровизация привела к появлению новых видов зависимостей. Цифровая зависимость базируется на том же физиологическом принципе, что и химическая зависимость. К видам цифровой зависимости относят: чрезмерное увлечение онлайн – играми; социальными сетями, киберсексуальная зависимость, а также неконтролируемый поиск любой информации в сети Интернет.

Ключевые слова: девиантное поведение, игромания, информационная зависимость, киберсексуализация, культ немедленного удовлетворения, синдром отвращения ожидания, цифровые аддикции, цифровое поколение

V.A. Shunyaeva
Candidate of Legal Sciences, Associate Professor
Derzhavin Tambov State University

Psychophysiological features of digital addictions in the digital generation

Abstract. The purpose of this article is to identify the problem of digital addictions among the digital generation, which contribute to their criminalization. Digitalization has led to the emergence of new types of addictions. Digital addiction is based on the same physiological principle as chemical addiction. The types of digital addiction include excessive use of online games, social networks, cybersex addiction, and uncontrolled search for any information on the Internet.

Keywords: deviant behavior, gambling addiction, information addiction, cybersexuality, the cult of immediate gratification, anticipation aversion syndrome, digital addictions, and the digital generation

Введение. Происходящие социальные трансформации, оказывают существенное влияние как на развитие общества в целом, так и на отдельную личность. Особенно это касается современных несовершеннолетних. К ним относятся представители цифрового поколения.

Особенностью представителей цифрового поколения стала гаджетозависимость. Наличие такого технического инструмента (телефон, планшет, компьютер, ноутбук и т. д.) дает иллюзию возможности безопасной коммуникации и способствует двойственному состоянию психики несовершеннолетнего. Постоянный доступ к указанным коммуникационным средствам создает некую иллюзию спокойствия, которая нарушается сразу при получении негатива из различ-

ных информационно-коммуникационных сетей, либо в случае лишения такого инструмента общения, у несовершеннолетнего возникает агрессия, тревожность, апатия, уныние, в том числе и суицидальные проявления. Это связано с тем, что такие технические возможности воспринимаются как источник базовой потребности человека в безопасности. Виртуализация общения, по мнению подростков, защищает их от реального столкновения с другими людьми. Так «идея «обратимости» событий в Интернете, вероятность их «откручивания назад» (а это могут быть и оскорбления) позволяют личности относиться к организации коммуникативного процесса менее ответственно, не переживая стыд, угрызения совести»[8].

Основная часть. Не стоит недооценивать влияние особенностей физиологического и психического развития человека в его криминализации. Мы считаем, что личность преступника имеет биосоциальную природу. А, значит, ее изучение должно быть многогранным и учитывать различные элементы. Затронем отдельные аспекты биопсихического развития человека, обусловливающих его отклоняющееся поведение.

Различного рода зависимости, в том числе и цифровые, изменяют психофизиологическую сущность несовершеннолетнего, влияя на его нейрофизиологию.

Особенности центральной и периферической нервной системы формируют типовые поведенческие реакции на тот или иной социальный раздражитель. Имея большую возбудимость и восприимчивость такие лица потенциально склонны к совершению общественно опасных поступков, так как их нервная система не может адекватно справиться с внешними и внутренними раздражителями. Частым проявлением такой реакции на стрессовую ситуацию являются жестокость, низкая эмпатия, отсутствие страха. Степень проявленности особенностей нервной системы также зависит от нейрофизиологической структуры человека: для одной будет свойственна быстрая вспышкообразная, порой аффектированная реакция, для другой отличительной чертой является длительный этап терпимости, с последующим выбросом колоссальной разрушительной энергии.

Рассмотренные физиологические особенности личности, в настоящее время претерпевают изменения под влиянием меняющейся цифровой реальности. «Исследование новых цифровых миров выявляет как специфику картины мира, ценностных и символических систем членов онлайн-сообществ, так и взаимосвязь формирования их идентичности и особенностей использования цифровых платформ»[3. С. 13].

Особенно интенсивно негативное нейрофизилогическое развитие протекает у молодежи [6]. Как видим, цифровые аддикции напрямую связаны с нейрофизиологическими и клинико-биологическими составляющими человека, от их уровня развития зависит, как склонность к цифровой зависимости, так и формирование такой зависимости.

К видам цифровой зависимости относят: чрезмерное увлечение онлайн-играми; социальными сетями, киберсексуальная зависимость, а также неконтролируемый поиск любой информации в сети Интернет [11].

Компьютерные игры стали неотъемлемым атрибутом современной жизни. Их количество, виды и направления могут удовлетворить любой интерес.

В первую очередь желание играть проявляется у детей, как неотъемлемая часть их развития и жизни. Однако, компьютерные игры не так безопасны. Проведение исследования этой аддикции выявило, что у страдающих выраженным психическим расстройством на почве онлайн игр проявляются спутанность сознания, гипнотический транс, потеря ориентации, галлюцинации, головные боли, ухудшение сна, компульсивные движения [7. С. 44-46].

Еще одним видом цифровой зависимости стали социальные сети, в которых несовершеннолетние также проводят значительное количество времени, вступая во всевозможные сообщества. Социальные сети формируют определенный паттерн поведения, зависящий от нейрофизиологических особенностей мозга. Цикл «стимул – награда» здесь реализуется через реакции в социальных сетях. Так, размещенные пост, фото и видео собирают различные реакции (лайки, комментарии, клики и т. д.), желание одобрения от своей группы принадлежности стимулирует выброс дофамина в мозг.

Киеберсексуальная аддикция проявляется в сексуальном интересе, который в целом является нормальным на этапе развития пубертатного возраста человека. Однако Интернет значительно расширяет возможности подростков в получении информации, в том числе и негативно влияющей на их развитие. Аддикция в области киберсексуальной зависимости характеризуется стремлением к уходу от реальности посредством «фиксации внимания на определенных видах деятельности с целью получения интенсивных эмоций» [4. С. 8]. Яркость, призывность, доступность, разнообразие порноиндустрии легко овладевают сознанием и желанием молодежи, приводя к потере интереса реальной жизни.

Однако специфика таких преступлений в значительной их латентности, объясняемой во многом тем, что «дети не всегда сообщают о произошедшем из-за страха перед родителями, из-за шантажа преступника, единожды получившего интимную фотографию малолетнего и манипулирующего им в дальнейшем, или по другим причинам» [5. С. 46].

Еще одним видом цифровой аддикции является информационная зависимость, проявляющаяся в неконтролируемой жажде новой информации независимо от содержания и источника подачи (чаще всего сети Интернет).

Поведенческая зависимость в виде неконтролируемого потребления информации очень опасна в своем развитии именно у подростков, так как за счет постоянного потока сведений они пытаются уйти от неудовлетворяющей их реальности, что в целом лишь усугубляет проблему. Чаще всего такая аддикция у подростков проявляется в том, что они сразу после пробуждения спешат взять тот гаджет, который дает им информацию, с ним же они и засыпают. На протяжении дня они более 300 раз берут свои цифровые приспособления, чтобы проверить есть ли какие-то новости, они находятся в постоянном «веб-серфинге» [9, 10].

Заключение. Период физиологического и психологического созревания у подростков является наиболее критическим. Погружая свой мозг в дофаминовые стимулы, несовершеннолетние приобретают долгосрочные негативные изменения, проявляющиеся в неправильном формировании социального интеллекта и собственной идентичности. Справиться с негативными появлениями цифровой зависимости в виде вины и самокритики подросткам помогает осо-

знание массовости этого явления – «так делают все», примеры аналогичного поведения в тех социальных группах, которым он принадлежит, а также поддержка этих групп и культивирование такого поведения.

Рассмотренные цифровые аддикции формируют культ немедленного удовлетворения, воздействия на психофизиологические особенности личности подростка, в результате формируя его агрессивно депрессивное состояние, проявляющееся либо в аутоагрессии, либо в агрессии в отношении других людей.

Список литературы

1. Белашева Х.В. Интернет-зависимость как предиктор формирования нарушений личности с различными типами межполушарных асимметрий // Знание. Понимание. Умение. 2015. № 1. С. 224.
2. Галимова Р.З., Минахметова А.З., Адигамова Э.Б. Профилактика зависимости от социальных сетей у подростков // Казанский педагогический журнал. 2020. № 5. С. 182-190.
3. Гафарова Ю.Ю. Цифровая антропология: установки и принципы // Человек в социокультурном измерении. 2022. № 2. С. 13.
4. Еременко В.В. Транскультурные особенности самосознания личности с аддиктивным поведением в подростково-юношеском возрасте: автореф. дис. … канд. псих. наук. М., 2007.
5. Захаров Н.Д. Современное состояние преступности, посягающей на половую неприкосновенность несовершеннолетних с использованием сети Интернет // Вестник Волгоградской Академии МВД России. 2021. № 2 (57). С. 46.
6. Lee J, Hwang JY, Park SM, et al. Differential resting-state EEG patterns as sociated with comorbid depression in Internet addiction. Progress in Neuro Psychopharmacology & Biological Psychiatry. 2014; 50:21-26. https://doi.org/10.1016/j.pnpbp.2013.11.016.
7. Малыгин В.Л., Цыганков Б.Д., Хвостиков Г.С. Патологическая зависимость от азартной игры: клиника и динамика психопатологических феноменов. Особенности личностных свойств, зависимых от азартных игр // Журнал неврология и психиатрия им. С.С. Корсакова. 2007. 3 (22). С. 44-46.
8. Третьякова В. С., Церковникова Н. Г. Цифровое поколение: потери и приобретения // Профессиональное образование и рынок труда. 2021. № 2. С. 57. https://doi. org/10.52944/PORT.2021.45.2.004
9. Целищева З.А. Актуальные вопросы информационной безопасности молодежи в условиях гибридной войны // Интерактивная наука. 2022. № 10 (75). С. 43-45.
10. Шайдукова Л.К., Рашитова Э.Л. Клинические, гендерные и возрастные аспекты интернет-зависимости // Казанский медицинский журнал. 2020. №2. С. 193-199.
11. Young K.S., Cristiano N.D.A. Internet addiction in children and adolescents: risk factors, assessment, and treatment. New York: Springer Publishing Company; 2017.

УДК 343.98

И. О. Антонов,
кандидат юридических наук, доцент,
Казанский (Приволжский) федеральный университет

Особенности применения нейросетей в выявлении и расследовании корпоративного рейдерства

Аннотация. В статье рассмотрены основные направления применения нейросетей для решения задач выявления и предварительного расследования корпоративного рейдерства как весьма специфической разновидности экономической преступности. Повышение эффективности противодействия криминальному рейдерству остается актуальной проблемой для отечественных правоохранительных органов. За последние годы способы корпоративного рейдерства видоизменились, преступники стараются приспособить уже известные криминальные схемы к меняющимся условиям, а также разработать новые, более совершенные с целью осуществления рейдерских захватов. Для реализации своих преступных замыслов организаторы захватов используют самые различные средства, в том числе и современные цифровые технологии. В этой связи криминалистическое обеспечение процедур выявления и предварительного расследования корпоративного рейдерства, безусловно, должно включать в свой состав рекомендации по использованию потенциала нейросетей.

Ключевые слова: искусственный интеллект, корпоративное право, корпоративное рейдерство, недружественное поглощение, нейросеть, преступление, расследование, цифровые технологии

I. O. Antonov,
Ph.D. of Legal Sciences,
Associate Professor,
Kazan (Volga Region) Federal University

Distinctive features of the use of neural networks in the detection and preliminary investigation of corporate raiding

Abstract. The article examines the principal avenues for deploying neural networks to address the tasks of detecting and conducting the preliminary investigation of corporate raiding, a highly specific subtype of economic crime. Enhancing the effectiveness of countering criminal corporate raiding remains a pressing challenge for Russia's law-enforcement authorities. In recent years, the methods of corporate raiding have evolved: offenders have sought to adapt well-known criminal schemes

to changing conditions, as well as to devise new, more sophisticated techniques for effecting raider takeovers. To implement their criminal designs, the organizers of such takeovers employ a wide range of means, including contemporary digital technologies. In this regard, the criminalistics support of procedures for the detection and preliminary investigation of corporate raiding should, as an integral component, include recommendations for leveraging the substantial potential of neural networks.

Keywords: artificial intelligence, corporate law, corporate raiding, hostile takeover, neural network, crime, investigation, digital technologies

Введение. Криминальное рейдерство в настоящее время остается одним из самых опасных экономических преступлений. Пожалуй, самой изощренной разновидностью криминального захвата с точки зрения продуманности криминального замысла и разнообразия использованных для его реализации средств является корпоративное рейдерство. Выявление такого рода преступлений и грамотная организация их предварительного расследования предполагает наличие в арсенале правоохранителя самых разнообразных цифровых инструментов, в том числе самых современных нейросетей. Их значительный потенциал может рассматриваться через призму решения широкого спектра задач как на стадии возбуждения, так и на стадии предварительного расследования уголовных дел о корпоративном рейдерстве. В частности, нейросети могут способствовать своевременному выявлению признаков подготовки корпоративного рейдерства, оказать существенную помощь в определении ключевых направлений расследования уголовного дела, а также в выборе тактических средств для производства следственных действий и др.

Основная часть. Криминальное рейдерство в России остается одной из опасных разновидностей преступлений в сфере экономики. Пик криминальной активности рейдеров в РФ пришелся на конец двадцатого и начало двадцать первого века. С тех пор отечественное рейдерство заметно видоизменилось, но цели остались прежними – сначала лишить жертву захвата самостоятельности, а затем использовать ее ресурсы в своих интересах. Способы криминальных захватов из так называемых «лихих 90-х» уже не всегда могут быть успешно реализованы рейдерами в наше время, в том числе благодаря принятию так называемых «антирейдерских» законов. Так, в конце 20 века поводом для банкротства предприятия с целью последующего осуществления его криминального захвата могла стать даже сравнительно небольшая сумма, чем и не без успеха тогда пользовались рейдеры. В наши дни подобную криминальную схему воплотить в жизнь стало гораздо сложнее [2].

Специалисты основными параметрами современного отечественного рейдерства справедливо считают следующие: 1) активность рейдеров становится заметнее когда экономика начинает испытывать кризисные симптомы – актуализируются различные полу или полностью криминальные схемы захватов;

2) предпочтительной целью рейдеров являются компании, оборот которых превышает 1 млрд руб, но данный критерий выбора может быть не единственным. В целеполагании рейдеров во главе угла может оказаться наличие привлекательной для них недвижимости в собственности или обладание уникальной

технологией ноу-хау. Иными словами, любой актив, который способен окупить затраты на рейдерскую атаку, может стать весомым поводом для криминального передела собственности; 3) выбору рейдерами цели захвата во многом способствует наличие уязвимостей в системах правовой и информационной защиты компании; 4) рейдеры существенно модернизировали арсенал средств для осуществления криминального захвата (корпоративное рейдерство в наши дни явно превалирует над силовым рейдерством). Предпочтение отдается эксплуатации лазеек в корпоративном праве, слабостей кредитной истории и текущего финансового положения компании, использованию в криминальных целях неоднозначных эпизодов в биографии топ-менеджеров и собственников, а также применению методов OSINT, корпоративного шпионажа, GR-менеджмента [12].

Характерной особенностью корпоративного рейдерства остается то, что оно, как правило, совершается организованной группой, в составе которой есть лица, имеющие нередко весьма высокую квалификацию в сфере экономики и права. В этой связи показательным примером, является уголовное дело о криминальных захватах недвижимости в городе Копейске Челябинской области. Организаторами рейдерства стали председатель третейского суда Челябинской области, начальник управления по имуществу и земельным отношениям мэрии Копейска, генеральный директор местного хлебозавода (глава ОПГ), начальник его юридической службы и еще, как минимум, один высококвалифицированный юрист. Рейдеры в результате своей криминальной деятельности завладели правами на двадцать один объект недвижимости, составляющий весь имущественный комплекс Копейского хлебозавода, а также кинотеатром, муниципальными объектами, торгово-офисными зданиями, квартирами, земельными участками и нежилыми помещениями в Челябинской, Курганской и Оренбургской областях. Для реализации криминального замысла рейдеры использовали подложные документы на объекты, а также фиктивные решения регионального третейского суда, которые в последующем представляли в суды общей юрисдикции для получения исполнительных листов о признании права собственности [11].

Точкой отсчета в создании криминалистической методики расследования корпоративного рейдерства стало обобщение опыта, полученного в ходе производства по первым в современной России уголовным делам о криминальных недружественных поглощениях. Учитывая, что в УК РФ не было и в настоящее время, к сожалению, нет самостоятельной статьи, предусматривающей уголовную ответственность за криминальное рейдерство, то следователи, расследуя дела названной разновидности экономических преступлений, креативно применяли, прежде всего, криминалистические рекомендации, разработанные для уголовного судопроизводства по делам о мошенничестве, о вымогательстве, о подделке документов, о внесении заведомо ложных сведений в реестры, о преступлениях в сфере компьютерной информации и т. п. (перечень типичных совершаемых в ходе рейдерского захвата преступных деяний).

Проблемам криминалистического обеспечения предварительного расследования рейдерства посвящен целый ряд научных работ отечественных криминалистов [6, 9, 15].

Значимым дополнением, в том числе и вышеназванных криминалистических рекомендаций, реализуемых в процессе уголовного преследования рейдеров, являются рекомендации по использованию современных цифровых технологий в процессе обнаружения и предварительного расследования корпоративного рейдерства.

Как известно, одним из общепризнанных законов развития криминалистики является «закон активного творческого приспособления достижений различных наук для целей судопроизводства» [5. С. 71]. Актуальные цифровые технологии никак не могли стать исключением из названного закона. Творческое преобразование достижений цифровизации для удовлетворения насущных потребностей уголовного судопроизводства в наши дни является более чем серьезным подспорьем в решении следователем самых различных задач как при инициировании уголовного преследования, так и при осуществлении предварительного расследования. Данный вывод более чем справедлив, если речь идет о привлечении лиц к уголовной ответственности за совершение преступлений в сфере экономики вообще, и за корпоративное рейдерство в частности.

В юридической литературе признано аксиомой, что цифровые технологии, в том числе и нейронные сети могут быть с успехом адаптированы для решения специфических криминалистических задач, в основе которых (решений) лежит разносторонний анализ материалов собранных в процессе доследственной проверки и предварительного расследования. Спектр возможного применения нейросетей весьма широк: анализ материалов уголовных дел для выявления следственных ошибок процессуального и тактического характера, вычленение из массива расследуемых дел признаков серийности, объединение преступлений по схожим признакам и др. [4. С. 49]. Нейросети способны создавать модели, способные выявлять закономерности в криминальных событиях, определять характеристики потенциальных преступников и выявлять ключевые факторы, влияющие на динамику развития следственной ситуации в этом контексте [16. С. 56]. Помимо этого, специалисты видят возможность использования нейросетей в управлении уголовно-процессуальными рисками, в рациональном распределении нагрузки в зависимости от компетентности и загруженности, в прогнозировании развития ситуаций; в отслеживании соответствия фактических действий и решений действующему законодательству, в выявлении индикаторов, которые могут указывать на нарушения уголовно-процессуального законодательства [17. С. 252].

Особую важность применения нейросетей в решении задач предварительного расследования неоднократно подчеркивалось руководством СК РФ. [10] Вместе с этим признается, что использование технологий искусственного интеллекта в работе органов предварительного следствия должно быть весьма осторожным и под жестким контролем человека. Тем более, что в правоприменительной практике СК РФ уже известен прецедент, когда имело место быть ошибочное процессуальное решение (впоследствии исправленное) на основе рекомендаций, сделанных искусственным интеллектом. [3]. В литературе описаны случаи, которые прямо показывают, что контроль за использованием нейросетей должен быть не только жестким, но и постоянным, а также квалифицированным [14].

Как подтверждение сложившегося понимания серьезных перспектив применения нейросетей в повышении эффективности деятельности органов предварительного расследования можно рассматривать заявления руководства ведомственных научных учреждений, в которых говорится о проведении интенсивных целенаправленных исследований, направленных на изучение возможностей использования нейросетей в установлении обстоятельств совершенных преступлений и причастных к ним лиц [8].

Способы корпоративного рейдерства, реализуемые в настоящее время, тщательно продуманы. Их содержание включает в себя такие действия и решения, которые на начальном этапе криминального посягательства не указывают явно на то, что злоумышленники приступили к осуществлению криминального передела собственности. В этой связи выявление попытки захвата не всегда возможно в рамках рекомендуемых процедур типовых проверочных действий, обычно осуществляемых компаниями и правоохранительными органами.

Нейросети в данном случае выступают как более «продвинутые» инструменты (имеющие большие шансы на обнаружение признаков криминального посягательства) по сравнению с уже «освоенными» в следственной практике. То есть можно говорить (одна из самых популярных трактовок содержания употребляемых терминов [1]) о потенциале использования в решении задач по выявлению корпоративного рейдерства ИИ-агентов (полностью проактивных автономных систем, способных самостоятельно принимать решения и выполнять задачи без постоянных инструкций) и ИИ-ассистентов с агентским функционалом (реактивных инструментов, выполняющих команды пользователя и частично способных к автономным действиям).

Вместе с тем направления для поиска значимой для выявления признаков корпоративного рейдерства сведений с использованием потенциала нейросетей фактически остаются теми же самыми (описаны в криминалистической литературе [7. С. 80-81]). В эпоху всеобщей цифровизации лишь смещаются некоторые акценты. Как вариант, действия направленные на обнаружение активности злоумышленников на черном рынке информации, с целью получения значимых сведений о предполагаемой жертве рейдерства, для дальнейшего их использования при подготовке и совершения криминальных деяний (например, факт размещения в теневом интернете заказа на взлом корпоративной почты намеченной жертвы рейдерства, факт использования злоумышленниками нейросетей, для подготовки посягательства и т. п.).

Нейросети могут быть востребованы для решения задач по выявлению субъектов рейдерского захвата. Ориентирами здесь могут служить мотивы, которые уже возникли или с большой долей вероятности могут возникнуть в силу самых разных причин у определенных лиц. Также особый интерес будут представлять лица, обладающие достаточными профессиональными компетенциями, которые либо сами могут инициировать корпоративное рейдерство, либо способны выступить в качестве исполнителей соответствующего заказа на криминальный захват.

Потенциал нейросетей для выявления признаков возможного рейдерского захвата может быть реализован в рамках проверочных действий в отношении контрагентов и клиентов.

Способ корпоративного рейдерства очень часто включает в себя получение информации «изнутри» намеченной жертвы захвата. Речь идет о сборе ценных сведений со стороны собственных сотрудников компании (завербованных рейдерами или внедренных в компанию) для подготовки и совершения рейдерства. Выявлению такого рода сотрудников могут способствовать нейросети, нацеленные на обнаружение подозрительной активности или нетипичного поведения у представителей так называемой группы риска (например, лица, обладающие в силу своего должностного статуса доступом к внутренней документации, имеющей критическое значение для сохранения самостоятельности потенциальной жертвы рейдерского захвата).

Выявление рейдерских захватов нередко невозможно без тесного взаимодействия государственных правоохранительных органов и частных структур, обеспечивающих экономическую безопасность бизнеса. В настоящее время нейросети находятся на вооружении как первой группы, так и второй из названных групп субъектов выявления. В этой связи очень важно грамотно координировать совместные усилия в применении нейросетей для последующего успешного использования результатов такого применения в процессе доказывания по уголовному делу. Например, специалисты Управления организации расследований Департамента безопасности Сбербанка признают, что во многих ситуациях искусственный интеллект не может заменить человека, поэтому экспертное мнение и оценка опытного специалиста по-прежнему играют критически важную роль. Результаты совместной работы такого тандема (нейросеть и специалист) в расследования инцидентов в Сбере в 2023–2024 годах выглядят достаточно убедительно: правоохранительными органами при содействии Сбера возбуждено 1022 уголовных дела, по которым еще до процессуального решения следователя были установлены подозреваемые; задержаны 2594 лица, причастных к совершению преступлений; 85,7% инцидентов в отношении банка раскрыты по горячим следам; по выявленным преступным схемам в отношении банка предотвращен ущерб на 7,45 млрд рублей [18].

В юридической литературе убедительно обосновано, что нейросети должны быть необходимыми составляющими в системе поддержки принятия решений следователя, которая выступает в качестве универсального инструмента, объединяющего в себе колоссальный объем разноплановых данных, обладающего аналитическим функционалом, позволяющего находить неявные связи при расследовании преступлений, а также выполняющего функции технического и логического контроля процессуальных документов [13].

Нейросети в настоящее время рассматриваются как необходимый помощник как в организации расследования уголовного дела в целом, так и в выборе оптимальных тактических средств при производстве следственных действий.

При расследовании корпоративного рейдерства нейросети могут стать серьезным подспорьем в выдвижении общих и частных версий, в определении последовательности принятия процессуальных решений, в подготовке и производстве следственных и иных действий, в определении особенностей взаимодействия с оперативно-розыскными органами, специалистами, экспертами,

представителями компании, которая могла стать или стала жертвой корпоративного рейдерства, а также со средствами массовой информации.

Выбор тактики производства следственных действий по делу о корпоративном рейдерстве с участием подозреваемых, обвиняемых и свидетелей во многом определяется их личностными особенностями. Результаты применения нейросетей в психологическом профилировании личности участников следственных действий могут способствовать определению следователем наиболее эффективных тактических приемов и комплексов для решения задач расследования. В частности, при прогнозировании линии поведения участника рейдерского захвата в процессе предварительного расследования, в определении статуса лица в организованной преступной группе рейдеров, в прогнозировании модели поведения рейдера при проведении следственного действия с его участием, в вероятности противодействия расследованию, а при его высокой вероятности в содержании такого противодействия и т. п.

Заключение. В завершении необходимо отметить, что применение нейросетей в решении задач по выявлению и предварительному расследованию корпоративного рейдерства (как правило, весьма сложному и объемному) способно существенно повысить эффективность деятельности следователя по уголовным делам названной категории. В наши дни достижение истины по уголовному делу о корпоративном рейдерстве трудно представить без использования современных цифровых технологий, в том числе нейросетей. В этой связи разработка криминалистических рекомендаций, направленных на наиболее рациональное использование нейросетей как на стадии возбуждения уголовного дела о корпоративном рейдерстве, так и на стадии его предварительного расследования в настоящее время и в ближайшем будущем останется весьма актуальным направлением в криминалистической науке.

Список литературы

1. Аникина М. От WeChat до MAX: повторит ли Россия путь Китая в погоне за ИИ-агентами // РБК. 2025. 4 сентября. URL: https://pro.rbc.ru/demo/68b5969c9a79470ae41e5ad0 (дата обращения 04.09.2025).

2. Баранова А. Судья Цветкова: Новые подходы ВС отвечают запросу общества на справедливость // Российская газета. 2025. 19 июня. URL: https://rg.ru/2025/06/19/reg-urfo/zakon-i-spravedlivost.html (дата обращения 01.09.2025).

3. Бастрыкин допускает применение ИИ в следствии только под контролем человека // Интерфакс. 2025. 19 мая. URL: https://www.interfax.ru/russia/1026425 (дата обращения 01.09.2025).

4. Бахтеев Д.В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Уголовный процесс и криминалистика. 2018. № 2. С. 43–49

5. Белкин Р. С. Криминалистическая энциклопедия. М.: БЕК, 1997. 342 с.

6. Бурынин С.С. Уголовно-процессуальные проблемы противодействия преступлениям, совершаемым преступными группами в ходе рейдерских захва-

тов имущества: автореферат дис. ... кандидата юридических наук: 5.1.4. Уголовно-правовые науки. Москва, 2024. 32 с.

7. Бычков В. Корпоративное рейдерство: подготовка и совершение // Противодействие преступлениям в сфере экономики: материалы Междунар. науч.-практ. конф. / под ред. А.И. Бастрыкина. М.: ЮНИТИ-ДАНА, 2015. С. 80-85.

8. Интервью руководителя НИИ криминалистики СК России А.А.Бессонова информационному агентству ТАСС // Официальный сайт СК РФ. 2021. 19 октября. URL: https://sledcom.ru/press/interview/item/1621439 (дата обращения 01.09.2025).

9. Особенности выявления, раскрытия и расследования рейдерских захватов имущественных комплексов: учеб.-метод. пособие / А.М. Багмет и др.; под ред. А.М. Багмета, В.В. Бычкова. М.: ЮНИТИ-ДАНА, 2017. 239 с.

10. Петрова Н., Козлов И. Бастрыкин: планируется интегрировать нейросети в процесс розыска лиц // Российская газета. 2025. 14 января. URL: https://rg.ru/2025/01/14/bastrykin-planiruetsia-integrirovat-nejroseti-v-process-rozyska-lic.html (дата обращения 01.09.2025).

11. Пинкус М. На Урале за аферы на 355 миллионов осудили чиновников и бизнесменов // Российская газета. 2022. 15 апреля. URL: https://rg.ru/2022/04/15/reg-urfo/na-urale-za-afery-na-355-millionov-osudili-chinovnikov-i-biznesmenov.html (дата обращения 01.09.2025).

12. Рензяев К. Враг у ворот: какие ИТ-инструменты помогут отбиться от рейдеров // РБК. 2020. 16 сентября. URL: https://pro.rbc.ru/demo/5f58d1359a7947758f9dea46 (дата обращения 01.09.2025).

13. Себякин А.Г. Искусственный интеллект в криминалистике: система поддержки принятия решений // Baikal Research Journal. 2019. Т. 10, № 4. DOI:10.17150/2411-6262. 2019.10(4).21.

14. Севастьянова Н., Сальникова Д. Алгоритм вины. Менеджеры в России стали использовать ИИ в корыстных целях // РБК. 2025 4 сентября. URL: https://pro.rbc.ru/demo/68b6a2cb9a794795ec250a2c (дата обращения 04.09.2025).

15. Степанов С. Д. Особенности расследования преступлений, связанных с незаконными захватами имущественных комплексов юридических лиц (рейдерство): автореферат дис. ... канд. юрид. наук: 12.00.12. Ростов-на-Дону, 2021. 26 с.

16. Хамидуллин Р.С. Криминалистическое обеспечение использования технологии искусственного интеллекта в раскрытии и расследовании преступлений // Полицейская и следственная деятельность. 2024. № 1. С. 55-67.

17. Чурикова А.Ю. Перспективы применения системы управления уголовно-процессуальными рисками в условиях цифровизации // Вестник Саратовской государственной юридической академии. №5(154). 2023. С. 248-253.

18. Эксперт Сбера рассказал о роли искусственного интеллекта в расследовании преступлений // Современные страховые технологии. 2024. 25 июня. URL: https://consult-cct.ru/ekspert-sbera-rasskazal-o-roli-iskusstvennogo-intellekta-v-rassledovanii-prestuplenij (дата обращения 04.09.2025

УДК 343.131

С. В. Зуев,
доктор юридических наук, профессор,
Южно-Уральский государственный университет
(национальный исследовательский университет)

Цифровая криминалистика и электронный уголовный процесс: взаимосвязь и соотношение

Аннотация. В статье проводится сравнительное исследование цифровой криминалистики и электронного уголовного процесса. Научно обосновывается роль и значение цифровой криминалистики в организационно-технологическом обеспечении электронного уголовного процесса. Утверждается, что правильно выстроенная взаимосвязь и соотношение данных отраслей знаний позволит выстаивать конструктивные связи и более эффективно использовать правовые механизмы, а также решать организационно-технологические задачи в доказывании по уголовным делам.

Ключевые слова: электронный уголовный процесс, цифровая криминалистика, цифровые следы, электронные доказательства, электронное уголовное дело, цифровые технологии, цифровизация

S. V. Zuev,
Doctor of Law, Professor,
South Ural State University
(National Research University)

Digital forensics and electronic criminal proceedings: interrelation and relationship

Abstract. The article provides a comparative study of digital forensics and electronic criminal proceedings. The role and significance of digital forensics in the organizational and technological support of electronic criminal proceedings is scientifically substantiated. It is argued that a correctly built relationship and ratio of these branches of knowledge will allow building constructive connections and more effectively using legal mechanisms, as well as solving organizational and technological problems in proving in criminal cases.

Keywords: electronic criminal proceedings, digital forensics, digital traces, electronic evidence, electronic criminal case, digital technologies, digitalization

Введение. Современное развитие права во многом обусловлено трансформацией общественных отношений и государственного устройства, происходящей в связи с переносом значительной их части в цифровую среду. Это, безусловно, отражается на все отрасли знаний, включая кримкогнитивные науки, к которым относится уголовный процесс и криминалистика. С учетом активного

внедрения в последнее время цифровых технологий в практику раскрытия и расследования преступлений, а также необходимости теоретического обоснования и законодательного регулирования деятельности органов расследования и оперативных служб в сети «Интернет», возникла необходимость проведения исследования, направленного на изучение соотношения цифровой криминалистики и электронного уголовного процесса. Такой подход позволит в дальнейшем более глубже понять их взаимосвязь и соотношение, выстраивать конструктивные связи и более эффективно использовать правовые механизмы, а также решать организационно-технологические задачи в доказывании по уголовным делам.

Основная часть. Цифровую криминалистику можно считать частной криминалистической теорией и в каком-то смысле неким продолжением традиционной, устоявшейся, криминалистики. В основе цифровой криминалистики лежит учение о цифровых следах, а также криминалистическое исследование компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей, имеющих значение для раскрытия и расследования преступлений [10]. Криминалистика и цифровая криминалистика сопоставимы по ряду критериев, среди которых: содержание, общая характеристика инструментальных аппаратов и тенденции их развития, ключевой понятийный аппарат [1. С. 71].

Электронный уголовный процесс представляет собой новое социально-правовое и информационно-технологическое явление, отвечающее современным вызовам преступности и включающее в себя такие системообразующие элементы, как: электронный документооборот; электронное межведомственное взаимодействие; широкое использование цифровых технологий; цифровые платформы; цифровой профиль участника; контрольные точки принятия решений. Данные элементы в той или иной степени могут быть востребованы при производстве по уголовным делам в электронном формате. Примером может служить опыт Республики Казахстан, где уже несколько лет успешно реализуется проект «Электронное уголовное дело» (е-УД) [4. С. 193; 6].

Интерес представляет формирование электронного уголовного дела в США, где используемая система CM/ECF (Case Management and Electronic Case Files) представляет собой «автоматизированный порядок получения судебных документов и предоставления онлайн-доступа к судебным заявлениям, ходатайствам, объяснениям сторон и иным документам по делу, подаваемым сторонами и юристами. Она предусматривает возможность поиска материалов судебного дела и документов в базе данных, исходя из номера и статуса дела, даты подачи документа, существа дела, наименования стороны и др.» [12].

Теоретически, работа с электронными документами в рамках уголовного дела может осуществляться и без цифровой платформы, но тогда не могут быть задействованы дистанционные формы проведения следственных действий, невозможна подача электронных документов онлайн и т.д. Положительным примером решения поставленных задач может служить опыт использования данных технологий в Республике Азербайджан [8].

Цифровая криминалистика и электронный уголовный процесс взаимосвязаны и это проявляется, прежде всего, в обнаружении и фиксации цифровых следов и дальнейшем их использовании в доказывании, в том числе в качестве электронных доказательств. Последние требуют законодательного закрепления относительно порядка их приобщения к делу, проверки и оценки как по отдельности, так и с учетом других имеющихся доказательств в материалах расследования [3. С. 49].

Участие специалиста также может быть связующим звеном между цифровой криминалистикой и электронным уголовным процессом, поскольку современные цифровые технологии, применяемые в обоих областях знаний, требуют соответствующего уровня подготовки [9]. Следователи, дознаватели и сотрудники оперативных подразделений, как правило, не обладают необходимыми компетенциями, а порой и не вправе самостоятельно осуществлять поиск цифровых следов и фиксировать их для дальнейшего использования в ходе расследования.

Часть 2 статьи 164.1 УПК РФ предусматривает обязательное участие специалиста при изъятии электронных носителей информации. Однако, этот вопрос остается дискуссионным [5], поскольку законодатель не дает четкого ответа, что относить к электронным носителям информации и возникают разумные сомнения в том, что необходимость приглашать специалиста имеется всегда. Возможно, в некоторых случаях следователь мог бы и самостоятельно осуществить изъятие.

Несмотря на очевидную взаимосвязь цифровой криминалистики и электронного уголовного процесса, между ними есть и существенные различия. Цифровая криминалистика в целом призвана обеспечивать расследование преступлений и оказывать помощь следователю, дознавателю и органам, осуществляющим оперативную работу, в решении поставленным перед ними задач. Данная сфера может регламентироваться подзаконными актами, в том числе утвержденными ими инструкциями. Сфера электронного уголовного процесса основана на применении норм уголовно-процессуального законодательства, где Уголовно-процессуальный кодекс имеет приоритетное значение в случаях обнаружения противоречий и пробелов в нормах права. Согласно ч. 1 ст. 7 УПК РФ субъекты, ответственные за принятие решений (суд, прокурор, следователь, орган дознания, начальник органа дознания, начальник подразделения дознания и дознаватель), не вправе применять федеральный закон, противоречащий УПК РФ.

Соотношение цифровой криминалистики и электронного уголовного процесса «сродни» сравнению самой криминалистики и уголовного судопроизводства, как части относительно целого. С учетом этого просматривается необходимость в реализации организационно-технологической функции цифровой криминалистики применительно к электронному производству по уголовным делам. Это проявляется, прежде всего в применении специальных средств при работе в цифровой среде органов предварительного расследования и оперативных служб, в разработке и внедрении современных методик раскрытия и рас-

следования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, включая сеть «Интернет» [11].

Как справедливо заметил, Д.В. Воронков «процессы цифровизации и неизбежно связанные с ней новые способы совершения преступлений ставят перед наукой задачу по стиранию границ между гуманитарными и техническими областями знаний» [1. С. 74]. В данном случае просматривается сближение физики и права [2], что, в свою очередь, влечет необходимость юристам осваивать дополнительные компетенции в области знаний технологий и процессов, происходящих на физическом уровне.

Заключение. Подводя итог, следует подчеркнуть важную роль цифровой криминалистики в решении организационно-технологических задач электронного уголовного процесса, поскольку уголовное судопроизводство на современном этапе нуждается в грамотном и повсеместном применении цифровых технологий, а значит в новых средствах и методах раскрытия и расследования преступлений, совершение которых сопровождается отражением преступных действий в цифровой среде.

Список литературы

1. Воронков Д. В. О соотношении традиционной криминалистики и цифровой криминалистики // Baikal Research Journal. 2025. Т. 16, № 1. С. 70-75.

2. Зуев С. В. Физика уголовного процесса: постановка проблемы // Правопорядок: история, теория, практика. 2022. № 1(32). С. 83-88.

3. Зуев С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение // Правопорядок: история, теория, практика. 2020. № 3(26). С. 46-51.

4. Информационные технологии в уголовном процессе зарубежных стран / Д. В. Бахтеев, В. А. Задорожная, А. И. Зазулин [и др.]. М.: Издательство «Юрлитинформ», 2020.

5. Костенко Р. В., Петрова О. А. Проблемы изъятия электронных носителей информации в отечественном уголовном процессе // Юридический вестник Кубанского государственного университета. 2021. № 1. С. 62-71.

6. Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. Электронно-уголовное дело (Е-УД). URL: https://www.gov.kz/memleket/entities/mdai/press/article/details/100226 (дата обращения: 07.09.2025).

7. Моругина Н. А. Зарубежный опыт использования электронного производства по уголовным делам // Вестник Пермского университета. Юридические науки. 2025. № 1(67). С. 117-143.

8. Моругина Н. А. Единая платформа E-Justice («электронное правосудие»): положительный опыт Азербайджанской Республики // Актуальные проблемы теории и практики уголовного процесса: Сборник научных трудов Международной научно-практической конференции, Ростов-на-Дону, 14 ноября 2024 г. Ростов-на-Дону: Ростовский юридический институт МВД РФ, 2025. С. 90-101.

9. Пастухов П. С. Роль и значение специальных знаний в информационно-технологическом обеспечении уголовно-процессуального доказывания // Вестник Пермского университета. Юридические науки. 2014. № 1. С. 298-304.

10. Цифровая криминалистика: учебник / В. Б. Вехов, С. В. Зуев, Д. В. Бахтеев [и др.]. 2-е издание, дополненное и переработанное. М.: Издательство Юрайт, 2024.

11. Электронное раскрытие и расследование преступлений / под ред. С. В. Зуева С.В., П. С. Пастухова. М.: «Юрлитинформ», 2025.

12. EVIDENCE.com расширяет свою облачную «Виртуальную комнату для сбора улик». URL: https://tracxn.com/d/companies/evidence.com (дата обращения: 07.09.2025).

УДК 343.98

А. А. Рясов,
кандидат юридических наук, доцент,
Ставропольский филиал Краснодарского университета
МВД России

Возможности поиска и исследования скрываемой информации на электронных носителях

Аннотация. Развитие современных информационно-коммуникационных технологий привело к кардинальному изменению структуры хранения и обработки данных, предоставив пользователям беспрецедентные объемы доступной памяти на различных цифровых устройствах. Одновременно с этими позитивными изменениями возникла новая категория угроз информационной безопасности, связанная с повышением риска несанкционированного доступа к персональным данным. Постоянное усовершенствование методов киберпреступников ставит перед владельцами информации задачу поиска надежных и эффективных способов защиты личных данных от посторонних лиц, включая родственников, знакомых и профессиональных злоумышленников. В поисках решения пользователи активно осваивают разнообразные техники шифрования и маскировки данных, основываясь на собственном уровне владения информационными технологиями. Однако парадокс заключается в том, что приобретенные знания и умения нередко находят применение не только в законных целях, но и в интересах криминальных субъектов, стремящихся надежно укрыть собственную запрещенную информацию от правоохранительных органов. Эта ситуация формирует серьезную проблему для правоохранительных структур, вынужденных повышать квалификацию своих сотрудников в вопросах выявления и анализа скрытых данных на цифровых носителях.

Ключевые слова: поиск скрытой информации, исследование электронных носителей, методы анализа данных, компьютерная криминалистика, шифрование информации, анализ метаданных, обнаружение стеганографии, крытые разделы диска, электронные носители данных

A. Ryasov,
Candidate of Law, Associate Professor,
Stavropol Branch of Krasnodar University of the
Ministry of Internal Affairs of Russia

The possibilities of searching and researching hidden information on electronic media

Abstract. The development of modern information and communication technologies has led to a fundamental change in the structure of data storage and processing, providing users with unprecedented amounts of available memory on various

devices, such as stationary and mobile electronic devices, removable drives and cloud services. Simultaneously with these positive changes, a new category of information security threats has emerged, associated with an increased risk of unauthorized access to personal data. The constant improvement of cybercriminal methods sets information owners the task of finding reliable and effective ways to protect personal data from unauthorized persons, including relatives, acquaintances and professional intruders. In search of a solution, users are actively learning a variety of encryption and data masking techniques based on their own level of knowledge of information technology. However, the paradox lies in the fact that acquired knowledge and skills are often used not only for legitimate purposes, but also in the interests of criminal actors seeking to reliably hide their own prohibited information from law enforcement agencies.This situation poses a serious problem for law enforcement agencies, which are forced to improve the skills of their employees in identifying and analyzing hidden data on digital media. Deep knowledge of the functioning of computer devices, the specifics of building file systems and modern methods of digital forensics contribute to solving this problem.

Keywords: hidden information search, electronic media research, data analysis methods, computer forensics, information encryption, metadata analysis, steganography detection, covered disk partitions, electronic data carriers

Введение. Информационно-коммуникационные преобразования в мире существенно трансформировали организационную структуру преступных сообществ, упростив процессы координации и коммуникации между участниками криминальных схем. Применение цифровых технологий позволило создать надежные и малозаметные каналы передачи информации, необходимые для планирования, реализации и последующей конспирации преступных деяний. Указанное обстоятельство объективно способствовало количественному росту сложных преступлений, отличающихся высоким уровнем латентности и значительной сложностью в установлении причастных лиц.

Одновременно с этим электронные следы, неизбежно возникающие в процессе цифровой коммуникации, формируют уникальную доказательную базу, необходимую для формирования обвинительного заключения против подозреваемых. Однако данное преимущество сопровождается необходимостью непрерывного совершенствования методов противодействия высокотехнологичным правонарушениям, поскольку наблюдаемая динамика показывает устойчивый рост числа преступлений, совершенных с использованием цифровых ресурсов.

Постоянное обновление и улучшение технологий хранения и передачи данных стимулирует появление новых, нестандартных подходов к сокрытию значимых сведений, существенно усложняющих проведение следственно-экспертных мероприятий. Таким образом, актуальной задачей современного правоприменения становится разработка и внедрение эффективных методик поиска, анализа и интерпретации скрытой информации, полученной посредством цифровых коммуникационных каналов.

Проблема усугубляется острым дефицитом квалифицированных специалистов в системе Министерства внутренних дел Российской Федерации, официально признанным министром Владимиром Колокольцевым. Формально предусмотренное законом обязательное присутствие специалиста при производстве следственных действий, связанных с изъятием цифровых носителей, сталкивается с практической нереализуемостью из-за ограниченной численности профессионально подготовленного персонала.

Проблемой поиска сокрытой информации отчасти затрагивали отдельные авторы такие как: Л. А.Бураева [1], В. А.Гаужаева [2], Р. Р. Карданов [3], Н. С. Зиновьева [4] и др. Однако в этом направлении делается лишь попытка привлечь внимание к данному вопросу, но полноценных работ, посвященных его рассмотрению практически нет.

В этой связи назрела потребность переосмысления существующей модели подготовки кадров в ведомственных образовательных учреждениях. Специфические компетенции в области поиска, анализа и оценки цифровых доказательств должны стать неотъемлемой частью базовой подготовки широкого спектра сотрудников правоохранительных органов, выйдя за пределы узкого круга специализированных подразделений. Реализация подобной инициативы потребует масштабных изменений в содержании образовательных программ, ориентированных на формирование глубоких знаний в сфере информационной безопасности.

Основная часть. Анализ и выявление скрытой информации на цифровых носителях представляют собой важную составляющую обеспечения информационной безопасности и предотвращения угроз различного характера. Методы обнаружения включают широкий спектр техник: начиная от анализа цифровых артефактов и проверки метаданных, заканчивая использованием специализированного ПО, аппаратных комплексов и продвинутых криптографических исследований.

Именно поэтому специалисты в областях информационной безопасности, криптологии и компьютерного расследования уделяют особое внимание разработке и внедрению новых подходов к обнаружению и изучению скрытой информации. Их усилия направлены на систематизацию знаний и разработку эффективных практик, позволяющих успешно противостоять современным вызовам в сфере кибербезопасности.

На сегодняшний день существует значительное разнообразие методов сокрытия данных, выбор которых определяется уровнем осведомленности субъекта, характером и степенью конфиденциальности скрываемой информации. Рассмотрим наиболее распространенные из них подробнее:

1. Перемещение данных в системные директории.

Простейший способ заключается в размещении файлов в стандартных системных папках, таких как «C:\Windows\System32\Com\dmp» или «C:\Users\<ИмяПользователя>\AppData\Local\Temp_avast_\unp_low». Цель состоит в том, чтобы скрыть информацию в местах, редко посещаемых обычными пользователями. Однако подобный подход легко распознается специалистами благодаря простоте обнаружения с помощью масок имен файлов и расширений.

2. Архивирование с защитой паролем.

Другой распространенный вариант – помещение данных внутрь защищенного паролем архива формата ZIP, RAR и аналогичных. Обнаружение самого архива не составляет труда, однако открытие содержимого требует наличия ключа. Подбор пароля возможен с использованием специализированного программного обеспечения («PassFab for RAR», продукты Elcomsoft и прочие утилиты), эффективность которого сильно варьируется в зависимости от сложности пароля и производительности используемого оборудования.

Отдельно отметим возникшие сложности, вызванные санкционными мерами ряда зарубежных стран, затруднившими легальное приобретение лицензий на зарубежные программные средства. Эксперты вынуждены искать отечественные аналоги или сотрудничать с частными организациями, имеющими доступ к необходимым инструментам.

3. Изменение атрибутов и наименований файлов.

Еще один несложный прием – модификация имени файла, расширение или установка атрибута «скрытый». Часто применяется совместно с предыдущими методами. Контрмерой служит тщательное сканирование по содержанию, датам модификации и прочим параметрам.

4. Создание визуально незаметных папок.

Создание папок с невидимыми символами в названии и заменой стандартной пиктограммы на прозрачную делает объект практически неразличимым на экране. Впрочем, выделение всей рабочей области мышью мгновенно демонстрирует наличие такой папки.

5. Удаление файлов.

Удаленная информация фактически сохраняется на физическом уровне носителя, пока не будет перезаписана новыми данными. Специальные приложения (например, «R-Studio», «Recuva», «Hetman Partition Recovery» и их аналоги) позволяют восстанавливать стертые материалы быстро и эффективно. Дополнительно полезно применять специализированные утилиты, способные извлекать миниатюрные копии изображений и видеозаписей, сохраняемых операционной системой Windows в каталоге «%UserProfile%\AppData\Local\Microsoft\Windows\Explorer».

6. Скрытые логические диски.

Одним из распространенных способов сокрытия данных является размещение информации на логических дисках, скрытых от операционной системы. Подобные операции выполняются с помощью специализированных программ, таких как «Hidden Disk» и «Secret Disk», а также встроенными средствами самой операционной системы Windows. Несмотря на кажущуюся надежность метода, современное программное обеспечение, используемое экспертами в рамках судебно-компьютерной экспертизы, позволяет без особых усилий обнаруживать и извлекать содержимое таких скрытых областей.

7. Стеганографические методы.

Стеганография представляет собой эффективный и сложный метод сокрытия информации, заключающийся в интеграции одних данных непосредственно внутрь других, таких как графические, аудиофайлы или видеоролики.

Информация внедряется таким образом, что визуальная или звуковая составляющая остается неизменной для обычного наблюдателя, однако специальная программа способна извлечь скрытое послание.

Примером служат программы: S-Tools, OpenPuff, RedJPEG, DeepSound и др.

Некоторые из указанных программ обладают дополнительными возможностями, такими как защита паролем и создание контейнеров с двойным дном, когда разные пароли обеспечивают доступ к различным наборам данных.

Несмотря на высокую степень надежности стеганографии, существуют программные комплексы, предназначенные для ее обнаружения и анализа, такие как: StegoHunt MP, Stegdetect, StegoWatch и др.

Эти инструменты способны определять вероятность наличия стеганографической информации в файле и предлагать возможные алгоритмы ее извлечения.

Также возможна элементарная форма стеганографии путем сокрытия текста внутри другого текста, например, изменением размеров шрифтов и цветовой гаммы в текстовых редакторах (например, MS Word). Однако подобная техника утрачивает свою эффективность при сохранении документа в текстовом формате (.txt).

8. Использование криптоконтейнеров и шифрование данных.

Самым надежным и одновременно наиболее сложным для судебного анализа методом считается использование криптоконтейнеров и шифрованных дисков. Закодированные файлы создаются специальными алгоритмами шифрования (AES, RSA и прочими), делая их содержание абсолютно недоступным без уникального ключа дешифрации.

Популярные программы для создания криптоконтейнеров: TrueCrypt, VeraCrypt и BitLocker.

Они позволяют создавать как одиночные контейнеры, так и контейнеры с двойной защитой (различные пароли открывают различное содержимое). Более того, криптоконтейнер может быть искусно замаскирован под совершенно иной тип файла, что дополнительно затрудняет его обнаружение.

Даже самые мощные программные средства, используемые экспертами (такие как): Passware Kit Forensic, Elcomsoft Forensic Disk Decryptor, John the Ripper, Hashcat далеко не всегда оказываются успешными, особенно если пароль подобран грамотно и обладает высокой стойкостью к взлому. В таких ситуациях единственным действенным инструментом остаются социальные методы воздействия и психологические приемы, направленные на получение пароля от владельца.

Помимо прямых методов обнаружения, важное значение имеет наличие косвенных признаков, позволяющих предположить наличие на электронном носителе скрытых данных. К ним можно отнести:

– Изменения в системных и временных файлах.

– Модификации реестра операционной системы.

– Установленные программы, характерные для сокрытия данных (например, VeraCrypt, TrueCrypt).

– Несоответствие объема файла заявленному типу файла.

– История запусков определенных программ и документов.

– Эскизы графических файлов, содержащих потенциально важные свидетельства.

Специальные инструменты, такие как EnCase Forensic и FTK Imager, оказывают значительную поддержку экспертам в выявлении подобных косвенных признаков.

Важно помнить, что само по себе наличие зашифрованных файлов или программ шифрования не обязательно связано с неправомерной деятельностью и требует внимательного и осторожного подхода при оценке.

Заключение. Таким образом, несмотря на существование множества высокоэффективных методов сокрытия информации, современная судебная экспертиза располагает широкими возможностями для их обнаружения и расшифровки. Успешность подобных операций напрямую зависит от профессионализма специалистов, качества используемого оборудования и программного обеспечения, а также своевременности и полноты проводимых экспертиз.

Для повышения эффективности работы правоохранительных органов настоятельно рекомендуется дальнейшее обучение сотрудников основам информационной безопасности, глубокое освоение современных методов анализа цифровых данных и активное сотрудничество с ведущими производителями специализированного программного обеспечения.

Список литературы

1. Бураева Л. А., Шогенов Т. М. Роль информационных технологий в обеспечении общественного порядка и общественной безопасности // Социально-политические науки. 2019. Т. 9. № 5. С. 190-192.

2. Курин А. А., Гаужаева В. А. Электронно-цифровые следыкак объекты криминалистической регистрации // Право и управление. 2023. № 7. С. 141-147.

3. Курин А. А., Карданов Р. Р., Евстифеева Е. П. Направления развития системы информационно-аналитического обеспечения раскрытия и расследования преступлений // Право и управление. 2022. № 8. С. 113-118.

4. Зиновьева Н. С. Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений: автореф… дис. канд. юрид. наук. Краснодар: 2021. 28 с.

УДК 343.1

Е. А. Селезнева,
кандидат юридических наук, доцент,
Российский университет адвокатуры и нотариата
имени Г. Б. Мирзоева

Цифровые следы преступлений, связанных с деятельностью религиозных организаций

Аннотация. В статье исследуются особенности формирования и исследования цифровых следов при совершении преступлений, связанных с деятельностью религиозных организаций. Анализируются современные подходы к выявлению и расследованию религиозных преступлений в условиях цифровизации общественных отношений. Рассматриваются специфические характеристики цифровых следов, оставляемых при использовании информационно-телекоммуникационных технологий в религиозной сфере. Предлагаются направления совершенствования криминалистического обеспечения расследования данной категории преступлений.

Ключевые слова: цифровые следы, религиозные преступления, киберпреступления, информационные технологии, криминалистика, религиозные организации, цифровая криминалистика

E. A. Selezneva,
PhD in Law, candidate of Law, Senior Lecturer,
Mirzoev Russian University of Advocacy and Notary

Digital traces of crimes related to the activities of religious organizations

Abstract. The article examines the peculiarities of formation and investigation of digital traces in crimes related to the activities of religious organizations. Modern approaches to the detection and investigation of religious crimes in the context of digitalization of social relations are analyzed. The specific characteristics of digital traces left when using information and telecommunication technologies in the religious sphere are considered. Directions for improving the forensic support for the investigation of this category of crimes are proposed.

Keywords: digital traces, religious crimes, cybercrimes, information technologies, forensics, religious organizations, digital forensics

Введение. Современное общество характеризуется стремительным развитием информационно-коммуникационных технологий, которые проникают во все сферы человеческой деятельности. Согласно актуальным статистическим данным МВД России за 2024 год, наблюдается устойчивый рост киберпреступности: число преступлений в ИТ-сфере достигло 765,4 тыс. случаев, что на 13,1% превысило показатели 2023 года. Доля киберпреступлений в общем чис-

ле зарегистрированных преступлений составила 40%, что является рекордным значением за последние пять лет. При этом объем ущерба от таких преступлений вырос на 36% и достиг 200 млрд рублей [8]. Религиозная сфера не остается в стороне от этих процессов, что обуславливает необходимость исследования специфических особенностей цифровых следов при совершении преступлений, связанных с деятельностью религиозных организаций.

Актуальность исследуемой проблематики определяется несколькими факторами.

Во-первых, религиозные организации все активнее используют цифровые технологии для осуществления своей деятельности, что создает новые возможности для совершения преступлений и одновременно формирует специфические цифровые следы.

Во-вторых, как справедливо отмечают исследователи, в современном геополитическом противостоянии различные деструктивные религиозные организации активно применяются для дестабилизации общества и вербовки агентов влияния [5].

В-третьих, существующие подходы к расследованию религиозных преступлений требуют адаптации к условиям цифровизации.

Основная часть. Анализ действующего законодательства позволяет констатировать, что в уголовном законе отсутствует не только раздел, но и глава, посвященная непосредственно религиозным преступлениям. Это создает дополнительные сложности при квалификации деяний, совершаемых с использованием цифровых технологий в религиозной сфере. Классификация преступлений, совершаемых с использованием цифровых технологий, может осуществляться по различным основаниям: по объекту преступления, по предмету преступления, по способу совершения [1].

Цифровые следы преступлений, связанных с деятельностью религиозных организаций, обладают рядом специфических характеристик. Прежде всего, необходимо отметить, что само понятие «цифровой след» в криминалистической науке находится в стадии формирования. Некоторые авторы предлагают для криминалистического обеспечения расследования преступлений, совершаемых с использованием компьютерных средств и систем, создать новую науку – «электронную криминалистику» [2]. Однако более обоснованной представляется позиция Е.Р. Россинской, которая считает, что криминалистика едина, имеет свой предмет, систему, задачи, объекты и изучаемые закономерности [6].

В контексте религиозных преступлений цифровые следы могут формироваться при различных обстоятельствах. Особое внимание заслуживает использование сети Интернет как средства и способа совершения преступлений. Развитие технологий позволяет говорить о становлении цифрового пространства в качестве особого места совершения преступления [4]. Стремительная цифровизация позволяет говорить о наличии такой части виртуального мира, не поддающейся физическим границам и территориальной целостности.

Специфика религиозных преступлений в цифровой среде проявляется в нескольких аспектах. Во-первых, религиозные организации используют информационные технологии для распространения своих идей, привлечения новых

последователей, координации деятельности. При этом могут создаваться цифровые следы, свидетельствующие о противоправном характере такой деятельности. Во-вторых, цифровые технологии могут использоваться для совершения традиционных преступлений, но с религиозной мотивацией или в религиозном контексте.

Анализ судебной практики показывает, что цифровые следы религиозных преступлений могут включать в себя различные виды электронной информации. К ним относятся электронные сообщения в мессенджерах и социальных сетях, содержащие призывы к экстремистской деятельности под религиозными лозунгами; записи телефонных разговоров, зафиксированные в цифровом формате; электронные документы, содержащие планы террористических актов или иной противоправной деятельности религиозных групп; данные о финансовых операциях, осуществляемых через электронные платежные системы для финансирования запрещенной деятельности.

Особого внимания заслуживает проблема использования современных технологий для склонения к совершению преступлений на религиозной почве. Интернет становится наиболее комфортным и легкодоступным инструментом поиска и склонения потенциальных жертв к противоправным действиям [7]. При этом формируются специфические цифровые следы, анализ которых позволяет выявить механизм совершения преступления и установить всех участников преступной деятельности.

Важным аспектом является использование цифровых технологий для распространения ложной информации о потерпевших, порочащей их честь и достоинство в информационно-телекоммуникационных сетях. В данном случае сеть Интернет одновременно выступает и средством совершения преступления, и способом его осуществления, поскольку само общественно опасное деяние совершается в сети и одномоментно она же облегчает передачу порочащей информации неограниченному кругу лиц [3].

Расследование преступлений, связанных с деятельностью религиозных организаций, в условиях цифровизации требует применения специальных методов и средств. Ключевое значение приобретает компьютерно-техническая экспертиза, позволяющая извлечь и проанализировать цифровые следы. Однако традиционные подходы к проведению такой экспертизы требуют адаптации с учетом специфики религиозных преступлений.

Существенные трудности возникают при работе с зашифрованной информацией, которая часто используется участниками религиозных экстремистских группировок для сокрытия своей деятельности. Современные методы шифрования создают серьезные препятствия для правоохранительных органов при попытках получить доступ к цифровым следам. В таких случаях особое значение приобретают косвенные данные, позволяющие установить факт наличия и характер скрытой информации.

Проблематичным остается вопрос о квалификации преступлений, совершаемых в цифровой среде религиозными организациями. Мошенничество, совершенное с использованием информационно-телекоммуникационных технологий под видом религиозной деятельности, может квалифицироваться по раз-

личным статьям УК РФ в зависимости от конкретных обстоятельств дела. При этом цифровые следы могут свидетельствовать как о способе совершения преступления, так и о его религиозной мотивации.

Значительную сложность представляет установление причинно-следственных связей между цифровыми следами и фактическими обстоятельствами преступления в религиозной сфере. Нередко между моментом создания цифрового следа и совершением преступления проходит значительное время, в течение которого информация может быть изменена или уничтожена. Кроме того, участники религиозных преступных группировок часто используют сложные схемы сокрытия своей деятельности, включая применение анонимизирующих технологий.

Международный характер многих религиозных организаций создает дополнительные проблемы при расследовании преступлений. Цифровые следы могут находиться на серверах, расположенных в различных юрисдикциях, что усложняет процедуры их получения и исследования. Необходимо развитие международного сотрудничества в сфере противодействия религиозным преступлениям, совершаемым с использованием цифровых технологий.

Перспективным направлением развития криминалистических методов исследования цифровых следов религиозных преступлений является применение технологий искусственного интеллекта и машинного обучения. Эти технологии могут существенно повысить эффективность анализа больших массивов цифровой информации, выявления скрытых связей между участниками преступных групп, прогнозирования их дальнейших действий.

Особое внимание следует уделить подготовке кадров для расследования религиозных преступлений в цифровой среде. Сотрудники правоохранительных органов должны обладать не только техническими знаниями в области информационных технологий, но и пониманием специфики религиозной деятельности, особенностей функционирования религиозных организаций в цифровом пространстве.

Необходимо также совершенствование нормативной правовой базы, регулирующей порядок работы с цифровыми следами религиозных преступлений. Действующее законодательство не в полной мере учитывает специфику таких следов, что создает препятствия для их эффективного использования в ходе расследования и в судебном разбирательстве.

Проведенное исследование позволяет сделать вывод о том, что цифровые следы преступлений, связанных с деятельностью религиозных организаций, представляют собой особую категорию криминалистически значимой информации, требующую специальных подходов к ее выявлению, фиксации, изъятию и исследованию. Специфика таких следов обусловлена как техническими особенностями их формирования и хранения, так и содержательными характеристиками, связанными с религиозным контекстом преступной деятельности.

Заключение. Эффективное противодействие религиозным преступлениям в цифровой среде требует комплексного подхода, включающего совершенствование законодательной базы, развитие криминалистических методов и средств, подготовку квалифицированных кадров, а также международное со-

трудничество. Только при условии реализации всех этих направлений можно обеспечить адекватный ответ на современные вызовы в сфере религиозной преступности.

Дальнейшие исследования в данной области должны быть направлены на разработку специализированных методик расследования конкретных видов религиозных преступлений, совершаемых с использованием цифровых технологий, создание автоматизированных систем анализа цифровых следов, а также на изучение психологических аспектов использования цифровых технологий в религиозной преступной деятельности. Поэтому дальнейшие исследования возможностей применения технологий искусственного интеллекта в уголовном процессе будут как никогда необходимы [9. С. 490].

Список литературы

1. Антипов Д. Н. Классификация преступлений, посягающих на религиозные отношения // Пробелы в российском законодательстве. 2018. № 7. С. 158-161.

2. Вехов В. Б. «Электронная криминалистика»: понятие и система // Криминалистика: актуальные вопросы теории и практики: сборник трудов участников Международной научно-практической конференции, Ростов-на-Дону, 25 мая 2017 года. Ростов-на-Дону: Ростовский юридический институт Министерства внутренних дел Российской Федерации, 2017. С. 40-46. EDN ZPTOTH.

3. Гаужаева В. А., Прокофьева Е.В., Прокофьева О. Ю. Преступность в сети Интернет: криминологические характеристики // Вестник экономической безопасности. 2019. № 4. С. 112-118.

4. Иванова Л. В., Пережогина Г. В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2020. Т. 6, № 4. С. 155-171.

5. Клюс В. В. Особенности противодействия религиозным преступлениям (криминотеологические аспекты) // Право Донецкой Народной Республики. 2020. № 3. С. 38-45.

6. Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. Москва: Норма, 2006. 656 с.

7. Туркулец В. А. Секстинг в отношении несовершеннолетних: уголовно-правовой и виктимологический аспекты // Юридические исследования. 2020. № 5. С. 1-11.

8. Ущерб от IT-преступлений в 2024 году вырос почти на 40% // ИА ТАСС. 2024. URL: https://tass.ru/obschestvo/23183001 (дата обращения: 04.09.2025).

9. Спиридонов М.С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481–497. https://doi.org/10.21202/jdtl.2023.20. EDN: acsqxh.

УДК 343.98

А. Б. Смушкин,
кандидат юридических наук, доцент,
ведущий научный сотрудник,
доцент кафедры криминалистики,
Саратовская государственная юридическая академия

Криминалистические аспекты изучения метавселенной

Исследование выполнено за счет гранта Российского научного фонда
№ 24-28-00312, https://rscf.ru/project/24-28-00312/

Аннотация. Статья содержит анализ отдельных криминалистических аспектов расследования преступлений, связанных с метавселенной. Автор предлагает трактовку пространства метавселенной как метапространства. Анализируются факторы, осложняющие расследование преступлений, связанных с метавселенной. Предлагается перечень основных источников криминалистически значимой информации. Автор предлагает отдельные технико- и тактико-криминалистические рекомендации, повышающие эффективность расследования рассматриваемых преступлений. Констатируется, что криминалистика в метавселенных требует комбинированного подхода: традиционная цифровая криминалистика плюс специфичные методы для пространственных/сенсорных данных, смарт-контрактов, децентрализованного хранения и криптовалютных следов. Подводя итог, отмечается, что развитие метавселенных развитие метавселенных меняет природу не только классических, но даже цифровых улик и требует сочетания специфических технических, правовых и организационных мер при расследовании преступлений. Подчеркивается важность надлежаще организованного взаимодействия с поставщиками интернет-услуг и операторами метавселенных.

Ключевые слова: право, цифровые технологии, метавселенная, криминалистика, преступления, компьютерно-моделируемая реальность, блокчейн, следственные действия в метапространстве

A. B. Smushkin,
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminalistics,
Saratov State Law Academy

Forensic aspects of studying the metaverse

Abstract. The article contains an analysis of individual criminalistic aspects of the investigation of crimes related to the metaverse. The author suggests an interpretation of the metaverse space as a meta-space. The factors complicating the investigation of crimes related to the metaverse are analyzed. A list of the main sources of

criminalistically significant information is proposed. The author offers separate technical and tactical-criminalistic recommendations that increase the effectiveness of the investigation of the crimes under consideration. It is stated that forensics in the metaverse requires a combined approach: traditional digital forensics + specific methods for spatial/sensory data, smart contracts, decentralized storage and cryptocurrency traces. To summarize, it is noted that the development of metaverses is changing the nature of not only classical, but even digital evidence and requires a combination of specific technical, legal and organizational measures in the investigation of crimes. The importance of properly organized interaction with Internet service providers and metaverse operators is emphasized.

Keywords: law, digital technologies, metaverse, criminology, crimes, computer-modeled reality, blockchain, investigative actions in the meta-space

Введение. Концепцию метавселенных можно назвать одной из самых интересных разработок конца 20 века. Утверждается, что в 2025 г. объем рынка метавселенной должен достичь 74,4 млрд долларов США, а количество пользователей уже к 2030 г. достигнет 2 633 млн пользователей [15].

Метапространство (пространство метавселенной) как специфических гибридный (человеко-машинный) элемент киберпространства направлено на реализацию своих интересов в компьютерно-моделируемом пространстве значительным количеством пользователей. М. Болл утверждает на счет метавселенной, что «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» [10]. Я.А. Климова подчеркивая физический аспект метавселенной указала, что «С криминалистической точки зрения метавселенная – это синкретизм физической, дополненной и виртуальной реальностей, образующих общее киберпространство» [5. С. 106].

Пространства метавселенной могут иметь различные способы сопряжения и протоколы безопасности. Мы уже ранее отмечали, что «метапространство нам представляется частным случаем воплощения киберпространства в визуализированном (а в перспективе и использующем иные органы чувств) виде, с возможностью пользователей коммуницировать между собой и с окружающим пространством через аватары» [8. С. 389]. При этом, указанное пространство характеризуется интерактивностью, многоуровневостью и динамичностью.

Различные варианты реализации метапространств становятся все более популярными, становясь платформами социальных, экономических, развлекательных и иных взаимодействий. Это приводит к новым вызовам для криминалистики. Опасность преступности в метапространстве осознается как в отечественном и зарубежном научном сообществе [2; 6; 11; 12; 14], так и отдельными странами [16] и межгосударственными организациями [3; 7]. В России судебно-следственная практика по делам, связанным с метавселенными, пока отсутствует. Зарубежная, прежде всего американская, практика характерна переносом ос-

новных концептов и трактовок (преступление, вина, стадии и т.д.) из «реального» мира. Однако Гомес-Кинтеро Джулиана (Juliana Gómez-Quintero), Шейн Д. Джонсон (Shane D. Johnson), Эрве Боррион (Hervé Borrion), Саманта Ландриган (Samantha Lundrigan), обоснованно отмечают, что «Несмотря на то, что существует большая неопределенность в отношении реальных преступлений, которые могут быть совершены в метавселенной, важно уже сейчас предвидеть возможные угрозы. Это может помочь заинтересованным сторонам, таким как правоохранительные органы, регулирующие органы, правительства и поставщики услуг, подготовиться к тому, что может произойти, и в идеале устранить такие угрозы до того, как появятся новые преступные схемы» [13].

Основная часть. Особенности инфраструктуры метавселенных – децентрализация, криптозащита, а также межплатформенная природа – осложняют работу правоохранителей, требуя новых технических, юридических и организационных подходов в криминалистике.

Нельзя не отметить ряд факторов, осложняющих расследование:

– Размещение большинства серверов и иных сервисов, с помощью которых осуществляется функционирование метавселенных и взаимодействия в них, на зарубежных площадках, что существенно осложняет расследование.

– Трансграничность большинства преступлений, связанных с метавселенными.

– Часто данные, связанные с метавселенными хранятся в распределенном виде с использованием блокчейн-технологий на площадках, находящихся в различных юрисдикциях.

Отсутствие четкого правового регулирования метавселенных. В.В. Денисович сомневается, «способны ли нынешние регулирующие органы в физическом мире эффективно регулировать метавселенную с помощью существующих законов и нормативных актов…» и отмечает, что «нет четкого ответа на вопрос: кто, как, какой государственный орган, в каком правовом статусе будет контролировать сами метавселенные, правовые отношения внутри метавселенной, правовые отношения, складывающиеся в результате использования пространства метавселенной, а также в отношении самой метавселенной» [1. С. 81].

Специфичность категории преступления для метавселенной (особенно с учетом разных национальных правовых режимов). «Возникает вопрос о том, как бороться с преступлениями, совершаемыми в виртуальной среде, и следует ли рассматривать их в рамках существующего деликтного или уголовного права, или же следует создать отдельную группу преступлений» [1. С.81].

Неопределенность статуса виртуального (в том числе- текенизированного с последующим переходом на NFT) имущества.

Анонимизация пользователей с помощью proxy-серверов, VPN, TOR. Пользователи могут присоединяться к определенному метапространству под псевдонимом, используя анонимные кошельки.

Необходимость трансфплатформенного расследования, обусловленная различными протоколами взаимодействия и форматами данных взаимосвязанных платформ метапространств.

Следователь должен владеть хотя бы минимумом знаний в области IT-технологий, криптографии, особенностей работы блокчейн-систем и иных технологий, применяемых в метавселенной.

С учетом того, что основная следовая картина преступлений, связанных с метавселенной носит цифровой характер, крайне важным будет оптимальное использование программно-аппаратных комплексов анализа электронных цифровых следов. При этом, следует учитывать, что, в отличие от материального места происшествия, киберпространство может быть изменено или стерто практически мгновенно, что требует оперативного снятия дампа памяти, а, в идеале и «снимка» всего участка метавселенной, где произошло событие.

Тактические приемы, используемые в ходе производства следственных действий при расследовании преступлений, связанных с метавселенной, должны быть направлены на максимальную эффективность, законность и безопасность следственных действий с учетом особенностей цифрового пространства и противодействия со стороны участников. Инструменты включают комбинирование методов классического уголовного процесса и цифровой криминалистики с прогнозированием развития ситуации и многоуровневым анализом данных.

Основными источниками криминалистически значимой информации по делам, связанным с метавселенной, могут выступать:

– компьютер и иные электронные устройства пользователя (3D-очки и др.). На них необходимо обращать внимание на файлы конфигурации, программы, предназначенных для обслуживания выхода в метавселенную, логи активности пользователя, кэш браузера, его историю, файлы и логи стороннего программного обеспечения;

– у провайдера интернет-услуг – логи активности пользователя и его IP-адрес, факты обращения к VPN-серверам и TOR. При этом следует принимать во внимание, что в последних случаях может быть отмечен только сам факт, без содержания действий и адресов, к которым обращался пользователь с помощью данных средств анонимизации;

– у провайдера метапространства – логи активности пользователя и его идентификаторы в виртуальных мирах, переписка в чатах виртуальных миров. Вообще при расследовании требуется глубокого сотрудничества с операторами метавселенных для применения специализированных технологий для мгновенной фиксации огромных объемов данных;

– платежные системы – данные о транзакциях пользователя, о владении цифровыми активами;

– в случае метавселенных, интегрированных с криптовалютами и NFT, транзакции можно отследить через публичные блокчейн-сети, что обеспечивает прозрачность и неизменность данных и т. д.

Поиск информации должен начинаться с цифровой среды программного комплекса платформы метапространства. Далее должно быть исследовано стороннее программное обеспечение и вспомогательные программные комплексы. После чего внимание следует уделить памяти и программному обеспечению устройств, обеспечивающих действия в метапространстве (3D-очки, манипуляторы, тактильные перчатки и т. д.). необходимо получить лог контроллеров,

данные движения/позиционирования, записи камер/микрофонов, конфигурации HMD (headset). Следует учитывать возможное изменение цифровой информации в ходе подобных исследований. Поэтому, обязательно применение блокираторов записи, а, в случае, более конкретного выявления носителя, на котором имеется криминалистически релевантная информация, снятие побитной копии и проведения любых исследований на ней, а не на оригинале. Кроме того, преступники могут использовать «приватные» или «зашифрованные» пространства внутри метавселенной, нестандартные протоколы или скрытые скрипты для коммуникации и хранения улик. Тактика предполагает поиск этих «подпространств» или анализ кода на наличие скрытых функций.

Как отмечают некоторые зарубежные ученые: «Учитывая взаимный эффект между Метавселенной и реальным миром, данные Метавселенной также могут содержать доказательства обычных преступлений в реальном мире. С другой стороны, информация из реального мира может дать подсказку при рассмотрении дела, которое имело место в Метавселенной. В некоторых случаях следователям придется изучать все данные из обеих вселенных и перемещаться между ними. Поэтому в Метавселенной нам нужны процедурные и технологические решения для цифровой криминалистики» [17].

Криминалистика в метавселенных требует комбинированного подхода: традиционная цифровая криминалистика + специфичные методы для пространственных/сенсорных данных, смарт-контрактов, децентрализованного хранения и криптовалютных следов.

С учетом того, что использование метапространств может как требовать установки программного клиента на компьютер пользователя, так и обходиться без него. платформы цифровых миров на основе клиента могут продуцировать больший объем необходимых цифровой криминалистике данных, получающих отражение в клиентском программном обеспечении и дополнительных файлах журналов.

Для расследования будет крайне важен интероперабельный подход. В ходе расследования крайне важна корреляция носящих мультимодальный характер данных различных типов и полученных из различных источников разных, взаимодействующих на основании различных протоколов платформ. С учетом объема продуцируемых данных, при расследовании рекомендуется применять методы анализа больших данных, а при использовании для транзакций в метавселенной платформ, основанных на блокчейн-технологии, блокчейн-аналитике.

Необходима мультиканальная корреляция, позволяющая связывать блокчейн-транзакции, сетевые логи и клиентские артефакты для установления событийной цепочки. Важной также будет трассировка происхождения и происхождения цифровых активов (provenance analysis): проверка цепочек владения NFT/цифровых предметов, контрактов и контрактных событий.

Следует также активно использовать построение социальных графов, отражающих связи между аккаунтами, групповые чаты, каналы и внешние ссылки (форумы, соцсети).

В рамках оперативно-розыскной деятельности возможно создание специализированного аватара для внедрения в виртуальные преступные сообщества (наркоторговцы, хакерские группы, экстремистские «культы»). Этот аватар должен быть разработан с учетом специфики сообщества: внешность, поведение, история.

Указанные методы позволят изучить закономерности механизма совершения преступления, идентифицировать IP- адрес и даже конкретного пользователя. При этом, идентификация пользователя кроме ключевых записей и IP-адресов может быть проведена по паттернам его поведения в метапространстве и аватарной самоидентификации. Аватарная самоидентификация связана с возможностью придать аватару любую внешность, а также совершать ими любые действия, пользуясь дистанционностью взаимодействия. Кроме того, изучается также ритм активности появления пользователя в метапространстве, стиль действий, манеру общения, особенности существования в метапространстве (конфликтность, мизантропность и т. д.). К поведенческим паттернам можно отнести: маршруты, скорость, траекторию передвижения аватара в цифровом мире, время начала и окончания сессий, интервал между ними, движения и жесты аватара, которые помогают идентифицировать уникальные поведенческие сигнатуры, скорость реакции. В ходе расследования желательно выявление мультиаккаунтов (нескольких аватар, регулируемых через 1 аккаунт) и ботов (программ автоматических действий аватара).

Для доказывания факта личных действий пользователя или «перехвата» аккаунта может быть использован анализ временных рядов (изменения поведения пользователя с течением времени, его сетевой активности и эффективности), а также исследование цифровых отпечатков электронных устройств пользователя (Device Fingerprint –«цифровой след, который сформирован в виде производного значения параметров, конфигурации программного и аппаратного обеспечения конкретного компьютерного устройства» [9. С. 292-304]). Следует также проанализировать временные метки- постараться сопоставить события в метапространстве и реальном мире.

Следователь обязательно должен предпринять меры для обнаружения прошедших стримов (трансляций) из метапространства, скриншотов (снимков экрана), которые часто осуществляют пользователи цифровых миров.

В случае выявления преступления, связанного с использованием уязвимостей или созданием вредоносных скриптов, желательно провести реверс-инжиниринг кода.

Особенности вербальных следственных действий могут быть связаны с необходимостью дистанционности их производства. Следует отметить, что ст. 189.1 УПК РФ фактически допускает использование систем только видеоконференц-связи, ограничивая единственным условием – технической возможностью. Однако представляется, что в перспективе при расследовании могут быть также применены технологии компьютерно-моделируемой реальности. Это может быть связано с необходимостью продемонстрировать следователю определенные действия, невозможные в реальном мире, но допущенные в виртуальном пространстве метавселенной, а также повышенными требованиями к

безопасности дающего показания на допросе или очной ставке свидетеля или потерпевшего. Установление личности лица, участвующего в следственном действии, в таком случае, будет проведено следователем-исполнителем, а аватару может быть придана любая внешность.

Нейроинтерфейс может помочь производству допроса в цифровом пространстве метавселенной лица, полностью парализованного. Однако на настоящий момент подобные технологии слишком дорогостоящие и представляются далекой перспективой.

Среди экспертиз, необходимость производства которых при расследовании преступлений, связанных с метаселенными, можно констатировать уже сейчас, в первую очередь, можно назвать все экспертизы вида компьютерно-технических: аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную экспертизы (данных), компьютерно-сетевую. В перспективе возможна потребность в новой экспертизе, учитывающей именно специфику метавселенной и блокчейна. Кроме того, полагаем перспективной экспертизу виртуальных активов, в задачи которой должны входить: анализ NFT/цифровых предметов, цепочка владения, происхождение активов, а также анализ экономических транзакций и потоков средств.

Активное развитие искусственного интеллекта и возможное его применение для обеспечение функционирования всей метавселенной или отдельных ее частей, а также обслуживание ИИ отдельных компьютерных персонажей метавселенной, существующих для фона или автоматической реализации определенного функционала при взаимодействии с пользователями (по аналогии с компьютерными играми их можно назвать – Мобы и NPC), дает предпосылки утверждать возможную необходимость в ближайшем будущем отдельного подвида компьютерно-технической экспертизы, анализирующей ИИ.

При обнаружении голосовых записей коммуникационных программ следует назначение фоноскопической экспертизы. Относительно оценки объектов виртуальной собственности В.И. Еремченко и О.В. Сафронкина отметили, что «Видится логичным отнести подобные исследования к классу судебно-экономических экспертиз и именовать их судебно-оценочной экспертизой (исследованием) стоимости объектов виртуальной собственности» [4. С. 67].

Заключение. Развитие технологического направления метавселенных ведет к дальнейшей виртуализации экономики, провоцируя трансформации в структуре производства, управлении, маркетинговой политике и экономике труда [18. С. 23]. Подводя итог можно отметить, что развитие метавселенных меняет природу не только классических, но даже цифровых улик и требует сочетания специфических технических, правовых и организационных мер при расследовании преступлений. Чтобы эффективнее расследовать преступления в этих средах, необходима координация между разработчиками платформ, экспертным сообществом и правоохранительными органами. Необходимо разработка протокола взаимодействия в области быстрых запросов провайдерам интернет-услуг и операторам самих метавселенных.

Список литературы

1. Денисович В. В. Криминологическое измерение метавселенных // Право и цифровые технологии: электрон. сб. ст. Междунар. науч.-практ. конф., Новополоцк, 24 ноября 2023 г. / Полоц. гос. ун-т им. Евфросинии Полоцкой; редкол.: И. В. Шахновская, П. В. Соловьев. Новополоцк: Полоц. гос. ун-т им. Евфросинии Полоцкой, 2024. С. 81-87.

2. Денисович В. В. Уголовно-правовые аспекты метавселенных // Технологии XXI века в юриспруденции: материалы седьмой международной научно-практической конференции, Екатеринбург, 05 июня 2025 года. Екатеринбург: АНО "Центр содействия развитию криминалистики «КримЛиб», 2025. С. 70-75.

3. Елизавета Антонова Е. Интерпол начнет расследовать преступления в метавселенных // Getblock. URL: https://getblock.net/news/interpol-will-startinvestigating-crimes-in-the-metaverse/ (дата обращения 30.07.2025).

4. Еремченко В.И., Сафронкина О.В. Проблемные вопросы определения суммы материального ущерба и пути их решения при расследовании мошенничества в сфере компьютерной информации в области индустрии компьютерных игр // Общество и право. 2019. №. 4 (70). С. 64-68.

5. Климова Я.А. Цифровая конвергенция в криминалистике// Вестник Волгоградской академии МВД России. 2024. № 4 (71). С. 105-110.

6. Коротковская, Е. В. Риски метавселенных и виртуальных пространств // Математическое и компьютерное моделирование в экономике, страховании и управлении рисками. 2022. № 7. С. 216-222.

7. Кузьмичева А. Интерпол столкнулся с проблемами определения преступлений в метавселенных//РБК URL: https://www.rbc.ru/crypto/news/63e1153c9a79475975128129?from=copy (дата обращения 30.07.2025).

8. Смушкин А. Б. Криминалистика и метапространство // Основные направления совершенствования системы национальной безопасности. 2023. № 3. С. 388-392.

9. Цифровая криминалистика: учебник / под ред. В.Б. Вехова, С.В. Зуева. 2-е изд., перераб. и доп. Москва: Юрайт, 2024. 490 с.

10. Ball M. The Metaverse: What It Is, Where to Find it, and Who Will Build It. 13.01.2020. URL: https://www.matthewball.vc/all/themetaverse (дата обращения 02.07.2025).

11. Copson N, Johnson S.D. A scoping review of metaverse-facilitated child sexual abuse// Social Sciences & Humanities Open, 2025, Volume 12, 101667.

12. Gómez-Quintero Juliana,. Johnson Shane D, Borrion Hervé, Lundrigan, Samantha A scoping study of crime facilitated by the metaverse// Futures, 2024, Volume 157, 103338.

13. Juliana Gómez-Quintero, Shane D. Johnson, Hervé Borrion, Samantha Lundrigan, A scoping study of crime facilitated by the metaverse// Futures, Volume 157, 2024, 103338.

14. Karapatakis Andreas Metaverse crimes in virtual (Un)reality: Fraud and sexual offences under English law// Journal of Economic Criminology, 2025, Volume 7, 100118.

15. Metavers- Worldwide//Statista URL: https://www.statista.com/outlook/amo/metaverse/worldwide?clckid=1e263a4c (дата обращения 02.07.2025).

16. Sam Shead Serious crime in the metaverse should be outlawed by the U.N., UAE minister says // CNBC. URL: https://www.cnbc.com/2022/05/25/metaversemurders-need-to-be-policed-says-uae-tech-minister.html (дата обращения 30.07.2025).

17. Shishir Kumar Shandilya, Yuvraj Singh, Ivan Izonin, Lesia Hentosh, Metaverse forensics framework: A NIST based investigation framework for metaverse// Science & Justice, Volume 64, Issue 6, 2024, P. 698-709.

18. Филипова И.А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7-32. https://doi.org/10.21202/jdtl.2023.1. EDN: LCCOJJ.

УДК 343.98; 004

А. М. Сосновикова,
стажер-исследователь,
Уральский государственный юридический университет
имени В. Ф. Яковлева

Биометрия в криминалистике: теория и практика

Исследование выполнено за счет гранта Российского научного фонда
№ 23-78-10011, https://rscf.ru/project/23-78-10011/

Аннотация. Работа посвящена рассмотрению некоторых технических и организационных проблем внедрения систем биометрической идентификации в деятельность по раскрытию и расследованию преступлений. Подробно описаны препятствия, связанные с предвзятостью населения, существенной коммерциализацией отрасли, а также с отсутствием профильных специалистов в правоохранительных органах. По результатам исследования делаются выводы о необходимости глубоко научного осмысления затронутых проблем и предлагаются пути их решения: просвещение граждан, привлечение научных коллективов, интеграция информационных систем и модернизация образовательных программ.

Ключевые слова: биометрия, биометрическая идентификация, единая биометрическая система, клавиатурный почерк, искусственный интеллект, цифровая трансформация, безопасность данных

A. M. Sosnovikova,
Junior researcher,
Ural State Law University named after V. F. Yakovlev

Biometrics in forensic science: theory and practice

Abstract. The article is devoted to the consideration of some technical and organizational problems of the implementation of biometric identification systems in the activities of solving and investigating crimes. The obstacles associated with public bias, significant commercialization of the industry, as well as the lack of specialized specialists in law enforcement agencies are described in detail. Based on the results of the study, conclusions are made about the need for a deep scientific understanding of the problems raised and ways to solve them are proposed: educating citizens, involving research teams, integrating information systems and modernizing educational programs.

Keywords: biometrics, biometric identification, unified biometric system, keystroke dynamics, artificial intelligence, digital transformation, data security

Введение. Развитие современных технологий придало новый импульс исследованиям в сфере криминалистической биометрической идентификации. Несмотря на то, что биометрия в таких ее направлениях как антропометрия, дактилоскопия и почерковедение на протяжении всей истории современной криминалистики играла значительную роль в раскрытии и расследовании преступлений, а появившиеся позднее фоноскопия и генетический анализ уже воспринимаются как традиционные методы идентификации преступников, весь потенциал биометрических данных далеко не раскрыт. Лишь в последние годы стали появляться технологические, нормативные и регуляторные предпосылки для этого, что и обусловило рост публикационной активности в областях, связанных с использованием биометрических данных для целей правоохранительной деятельности. Так, если в 2014 году в России было опубликовано 23 научные работы по соответствующей тематике, в 2019 – 111, то в 2024 – уже 279.

Вместе с тем, несмотря на очевидный научный интерес, практика все еще не использует большую часть биометрических технологий, и даже обработка «традиционных» биометрических свойств личности сталкивается с существенными препятствиями. В результате сегодня можно наблюдать негативную тенденцию все большего отдаления теории от практики, что чревато стагнацией развития прикладной криминалистики, когда, не будучи способной отследить и адаптировать к полевому использованию все актуальные рекомендации, она замкнется на достигнутом к текущему моменту уровне развития. Рассмотрим данную проблему более детально.

Основная часть

Практические проблемы реализации биометрической идентификации. Подавляющее большинство научных работ сегодня безусловно верно описывают преимущества биометрической идентификации для раскрытия и расследования преступлений. В качестве основных называются: высокая точность идентификации; сложность подлога данных; уникальность биометрических сведений; их доступность для визуального, в том числе удаленного, восприятия; высокая скорость получения результатов и т. д. [2; 7; 9. С. 109-110].

Вместе с тем, как было указано в начале работы, рассмотренные в науке возможности биометрии сегодня оказываются почти недоступными для практики, что связано со следующими, как представляется, главными причинами.

Отсутствие доверия у населения. Так, для того чтобы биометрическая идентификация приносила действительные результаты, необходимо наличие в государственной базе данных образцов значительной части населения, особенно если предполагается использование алгоритмов машинного обучения, которые требуют для правильной настройки большие данные. Однако многие люди опасаются потенциальных утечек данных, злоумышленного их использования или не желают предоставлять дополнительную информацию о себе государству.

Сегодня ведется активная политика, направленная на разрешение такой негативной предубежденности. Публикуются просветительские материалы, обосновывающие безосновательный характер отдельных опасений граждан [4]; разрабатываются инструменты ускоренной реализации прав и интересов граждан при использовании биометрических технологий (оплата улыбкой, дистан-

ционное восстановление доступа к сервису «Госуслуги», дистанционное ускоренное подтверждение банковских переводов на крупные суммы и пр.). Вместе с тем нередко заявленная добровольная биометрическая регистрация становится добровольно-принудительной: многие банки не дают пользователю возможности выбора в части представления своих изображения лица или записи голоса либо проставляют согласия на сбор и обработку биометрических данных в договорах банковского обслуживания по умолчанию, что не обладающий юридическими компетенциями или квалификацией в области информационной безопасности человек может и не заметить; кроме того, после отказа в предоставлении собственных биометрических данных заинтересованные субъекты начинают реализовывать настойчивую кампанию по убеждению пользователя в ошибочности ранее принятого решения, которая нередко оказывается результативной. Мы не будем оценивать этическую сторону подобного рода мероприятий, лишь подчеркнем, что они имеют двоякое значение: безусловно, цель биометрической регистрации максимального процента населения достигается, однако внутреннее отношение людей при этом меняется незначительно.

Однако необходимо констатировать, что объективно многие опасения граждан не являются обоснованными: в отличие от частых утечек таких персональных данных, как имя, место жительства, контактный номер телефона и пр., в России пока не зарегистрировано ни одного случая утечки биометрических персональных данных, что связано с повышенной степенью их защиты, а также с исключительно централизованным хранением в государственных базах данных [3], а не множественным дублированием у различных частных лиц.

Высокий уровень коммерциализации отрасли. Востребованность систем биометрической идентификации за счет скорости, удобства и надежности их применения приводит к постоянному росту рынка биометрических технологий [8], создание и реализация которых обеспечивают значительную прибыль, хотя и требуют достаточно существенных ресурсных затрат, в том числе работы профильных специалистов. В этой связи на практике государство находит подрядчика, который будет предоставлять свои разработки в области систем биометрической идентификации заинтересованным органам на коммерческой основе. Наиболее показательным примером данной ситуации и проблем, связанных с описанной моделью, является область дактилоскопической регистрации, где используется АДИС «ПАПИЛОН». Высокая стоимость последних версий программы, оснащенных модулем искусственного интеллекта, обеспечивающим значительно более эффективное (в частности, с позиций скорости и точности решения задач) установление тождества, нежели предшествующие версии, а также личный конфликт представителей обеих сторон создали ситуацию, когда подразделения МВД России имеют в своем распоряжении версии программы, отстающие на два поколения от актуальной, а процесс обучения операторов АДИС обеспечивается лишь фактом работы в правоохранительных органах опытных сотрудников, способных передать свои знания новым поколениям.

Однако подчеркнем, что биометрическая регистрация по изображению лица и записи голоса, развивающаяся в последние годы, реализуется по более оптимальной модели. Так, государство, используя фактор значительной попу-

лярности лицевой и голосовой биометрии в коммерческом секторе, обязало всех участников рынка предоставлять соответствующие данные пользователей в единую государственную систему. Таким образом, с одной стороны, в распоряжении государства оказывается значительно больше биометрических профилей, нежели чем в ситуации сбора данных собственными силами (через системы правоохранительных органов). С другой стороны, государство может полностью контролировать сохранность данных, порядок их использования и актуализацию методов обработки. Однако сегодня эта модель тоже не лишена недостатков, так как прямой интеграции информационных систем правоохранительных органов с Единой биометрической системой нет, сведения из нее получаются лишь посредством направления запросов, что осложняет и замедляет ее использование в целях раскрытия и расследования преступлений.

Отсутствие квалифицированных специалистов, способных выступить операторами биометрических систем. Использование любой узкоспециализированной технологии требует от человека соответствующего навыка, однако если использованию АДИС «ПАПИЛОН» ранее обучали представители компании-разработчика, а сейчас – прошедшие это обучение в свое время действующие сотрудники правоохранительных органов; генетический анализ осуществляется специалистами и экспертами в области биологии и медицины; то для новых направлений биометрической идентификации квалификации действующих сотрудников недостаточно.

В наиболее благоприятных случаях изучения внешности, голоса, рукописного почерка в системе правоохранительных органов можно указать на экспертов по соответствующим направлениям криминалистических исследований, которым достаточно пройти повышение квалификации, обучившись применять в своей экспертной практике новые специальные технические средства. Однако для исследования клавиатурного почерка, радужной оболочки глаза, рисунка вен и т. п. требуются более специфические познания, обучение которым не проводится, что вполне обоснованно – в нем отсутствует прикладная значимость, так как системы обработки этих биометрических данных не внедрены в практику. Однако это формирует «порочный круг»: для внедрения новых биометрических технологий нет специалистов, готовых их развивать, а подготовка специалистов не является целесообразной из-за отсутствия технологий.

Кроме того, распространение биометрических технологий создает возможность их оперативного использования следователем, дознавателем или оперативным сотрудником. Однако, чтобы они могли в действительности обращаться к рассматриваемым достижениям научно-технического прогресса, важно обеспечить их предварительное обучение не только основам применения конкретных программных и программно-аппаратных модулей, но и навыкам определения границ допустимого обращения к системам искусственного интеллекта (так как большинство современных биометрических систем функционируют именно на основе данной технологии). В противном случае биометрия не сможет получить полноценной реализации в правоохранительной сфере, так как действующие сотрудники просто не будут понимать, как правильно реализовывать взаимодействие с ней. Весьма показательным здесь является пример

задержания в 2023 году ученого А. И. Цветкова и применения к нему мер пресечения на основе решения системы лицевой биометрии, определившей его совпадение с личностью преступника с вероятностью 55 %. Представляется, что вдумчивая интерпретация результата, его перепроверка иными, в том числе экспертными методами, позволила бы избежать допущенной человеческой ошибки.

Мы рассмотрели три наиболее существенные, на наш взгляд, организационно-технические проблемы, которые сегодня стоят на пути широкой имплементации биометрических технологий в правоохранительную деятельность. Безусловно, данный список может быть продолжен такими немаловажными факторами, как угроза дипфейков, трудности импортозамещения и создания собственных комплексов по новым направлениям биометрии, постоянно присутствующая опасность нарушения режима защиты информации и пр. Однако указанные проблемы уже достаточно широко рассмотрены в науке [1, 5, 6], поэтому мы не будем углубляться в их описание.

Заключение. Резюмируя сказанное выше, подчеркнем, что несмотря на высокую роль прогностической функции науки, такие прикладные ее отрасли как криминалистика не должны существенно отрываться от практики. Исследуя темы, связанные с использованием биометрии, безусловно, критически важно демонстрировать тот положительный эффект, который она проявит в деятельности по раскрытию и расследованию преступлений, однако не менее важно выявлять существующие препятствия, стоящие на пути ее внедрения в эту деятельность, и предлагать пути их преодоления.

Сформулируем возможные методы разрешения рассмотренных выше проблем.

Преодоление недоверия и предвзятого отношения граждан, в первую очередь, может осуществляться через просвещение. Причем помимо абстрактных призывов, положительную роль могут сыграть:

а) апелляция к референтной группе (блогеры, актеры, политические деятели должны собственным примером показывать, что они доверяют государству хранение их биометрических персональных данных);

б) апелляция к статистике (открытое опубликование сведений о том, сколько преступлений было предотвращено благодаря базам биометрических данных, а также о успешно пресеченных попытках их взлома).

Одновременно с этим, несмотря на их безусловную эффективность, считаем недопустимым использовать прямо или косвенно принудительные меры, когда доступ к каким-либо услугам (использование телефонной связи и Интернет-соединения; регистрация в социальных сетях; получение кредита; поступление в образовательные учреждения и т. д.) будет полностью блокироваться или существенно затрудняться (в том числе посредством замедления) для тех, кто не предоставит свои биометрические данные.

Во-вторых, важно создавать надежную систему гарантий, благодаря которым граждане будут уверены не только в безопасности своих персональных данных, но и в том, что их хранение у государства действительно способно обеспечить защиту самого человека, его близких от преступных посягательств.

Проблема коммерциализации может быть решена через привлечение для разработки биометрических систем научных коллективов на основе грантового финансирования, а для поддержания, обновления и эксплуатации созданных таким образом комплексов – через создание собственных инженерно-исследовательских центров, в том числе в рамках расширения сферы действия Центра биометрических технологий, являющегося оператором Единой биометрической системы. Одновременно с этим считаем возможным обеспечить прямую интеграцию ведомственных информационных систем с базами данных Единой биометрической системы для исключения чрезмерной бюрократической нагрузки.

Наконец, проблема отсутствия специалистов может быть решена, помимо курсов повышения квалификации по отдельным направлениям, несущественной переработкой образовательных программ высшего юридического образования по дисциплинам криминалистического цикла, посредством включения в них отдельных курсов или тем, а также – структурных компонентов внутри профильных тем, посвященных вопросам прикладного использования биометрических технологий. Причем очень важно в данном случае уделять внимание не только теоретическим вопросам (в частности правилам оценки результата работы интеллектуальной системы поддержки принятия решений), но и практике работы с программными и программно-аппаратными комплексами. Безусловно, обеспечить соответствующую материально-техническую базу для каждого высшего учебного заведения не представляется сегодня возможным, однако вполне допустимо моделировать ситуации применения специализированных технологий через виртуальные криминалистические полигоны (очки дополненной реальности), а также организовывать мастер-классы с представителями разработчиков.

Представляется, что планомерное, но при этом оперативное разрешение рассмотренных в работе проблем позволит реализовать потенциал биометрической идентификации в деятельности по раскрытию и расследованию преступлений с наибольшей эффективностью. Однако для этого необходимо приложить значительные совместные усилия научного сообщества, сотрудников правоохранительных органов, государства и разработчиков биометрических технологий.

Список литературы

1. Бодров Н. Ф., Лебедева А. К. Развитие судебной экспертизы в эпоху дипфейков // Судебная экспертиза: прошлое, настоящее и взгляд в будущее: Материалы международной научно-практической конференции, Санкт-Петербург, 16–17 мая 2024 года. Санкт-Петербург: Санкт-Петербургский университет МВД РФ, 2024. С. 48–52.

2. Низаева С. Р. Возможности биометрии в криминалистической идентификации личности // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2024. № 24. С. 165–166.

3. Постановление Правительства РФ от 21.06.2024 № 834 «Об определении организации, осуществляющей функции оператора единой биометрической

системы» // Собрание законодательства Российской Федерации. 2024. № 26. Ст. 3672.

4. Сундукова Ю. 7 мифов о биометрии: разбираем с экспертом // РБК. Тренды. Индустрия 4.0. 2021, 9 сентября. URL: https://trends.rbc.ru/trends/industry/6139b6a69a7947ca4e744848 (дата обращения: 21.08.2025).

5. Amerini I., Barni M., Battiato S. [et al]. Deepfake Media Forensics: Status and Future Challenges // Journal of Imaging. 2025. Vol. 11 (3). No. 73. DOI: 10.3390/jimaging11030073.

6. Bhatt S., Sehrawat J., Gupta V. A systematic review of iris biometrics in forensic science: applications and challenges // Egyptian Journal of Forensic Sciences. 2025. Vol. 12. DOI: 10.1186/s41935-025-00431-7.

7. Pasupuleti M. Kr. Advanced Biometric Technologies in Forensic Science: Tools for Precision Identification and Investigation // International Journal of Academic and Industrial Research Innovation (IJAIRI). 2024. Vol. 4. No. 4. Pp. 131–139. DOI: 10.62311/nesx/932168.

8. Zoting Sh., Shivakar A. Biometric Technology Market Size, Share, and Trends 2025 to 2034 // Precedence Research. 2025, May 9. URL: https://www.precedenceresearch.com/biometric-technology-market (accessed: 21.08.2025).

9. Рахметов Б., Хайзабеков К. Поведенческая биометрия в Европейском союзе: правовые вызовы и технологические перспективы // Journal of Digital Technologies and Law. 2025. Т. 3, № 1. С. 108–124. https://doi.org/10.21202/jdtl.2025.5. EDN: joupzt.

УДК 343.9

Э. Г. Хомяков,
кандидат юридических наук, доцент,
Удмуртский государственный университет

Метаданные как составляющая цифрового следа в криминалистике

Аннотация. Статья посвящена анализу метаданных как элемента цифрового следа в криминалистике. В условиях цифровой трансформации правоохранительной деятельности метаданные становятся ключевым источником информации, позволяющим установить хронологию событий, местоположение участников и технические параметры их цифровой активности. В статье предлагается концепция, в которой метаданные рассматриваются как неотъемлемая составляющая цифрового следа, который, в свою очередь, формирует цифровое доказательство. Дается авторское определение понятия «метаданные» с позиций криминалистики и уголовного процесса, в котором они рассматриваются как технически фиксируемые сведения, образующие цифровой след. Подчеркивается необходимость нормативного закрепления понятий «цифровое доказательство», «цифровой след» и «метаданные» в единой правовой системе с учетом отечественных и международных стандартов.

Ключевые слова: метаданные, цифровой след, цифровое доказательство, телеком-метаданные, цепочка хранения, компьютерно-техническая экспертиза, допустимость доказательств

E. G. Khomyakov,
Candidate of Law, Associate Professor,
Udmurt State University

Metadata as a component of the digital trace in forensic science

Abstract. The article is devoted to the analysis of metadata as an element of the digital trace in forensic science. In the context of digital transformation of law enforcement, metadata have become a key source of information, allowing to establish the chronology of events, the location of participants, and technical parameters of their digital activity. The article proposes a concept in which metadata are considered an integral component of the digital trace, which, in turn, forms digital evidence. An author's definition of the concept of "metadata" is provided from the standpoint of criminology and criminal procedure, where they are viewed as technically recorded information forming a digital trace. The necessity of legally establishing the concepts of "digital evidence", "digital trace", and "metadata" within a unified legal system, taking into account national and international standards, is emphasized.

Keywords: metadata, digital trace, digital evidence, telecom metadata, chain of custody, computer-technical expertise, admissibility of evidence

Введение. Современные преступления редко совершаются без использования цифровых устройств, к которым можно отнести компьютеры, серверы, смартфоны, планшеты, цифровые камеры, видеорегистраторы, цифровые носители данных (жесткие диски, SSD-накопители и др.) и т.д. Цифровые устройства являются разновидностью электронных устройств, которые также могут быть аналоговыми [3. С. 73]. В подобных случаях ключевую роль в установлении истины по делу играют не только содержание переписки или файлов, но и метаданные – информация о данных: время, место, устройство, IP-адрес, геолокация, тип файла, маршрут передачи и другие технические параметры. Метаданные позволяют установить контекст происходившего, реконструировать хронологию событий и подтвердить или опровергнуть алиби подозреваемых.

Однако, несмотря на их высокую доказательную ценность, метаданные не обладают самостоятельным правовым статусом в российской правовой системе. Они напрямую не упоминаются в уголовно-процессуальном законодательстве. На практике они используются как составляющие вещественных доказательств (ст. 83 УПК РФ), к которым относятся «любые предметы: 1) которые служили орудиями, оборудованием или иными средствами совершения преступления или сохранили на себе следы преступления; 2) на которые были направлены преступные действия; … 3) иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела». Электронные носители (телефоны, флешки, жесткие диски) изымаются именно как указанные предметы. Результаты анализа метаданных фиксируются в заключении эксперта (ст. 204 УПК РФ), например, по компьютерно-технической экспертизе.

Проблема заключается в том, что само понятие «цифровое доказательство» отсутствует в Уголовно-процессуальном кодексе Российской Федерации. Это означает, что нет ни определения, ни классификации, ни специальных правил обращения с информацией, хранящейся в цифровой форме. Существующие виды доказательств, закрепленные в статье 74 УПК РФ (вещественные доказательства, протоколы следственных действий, заключения экспертов), не отражают особенностей цифровых данных – их волатильности (способности быстро изменяться или исчезать), возможности модификации, необходимости фиксации хэшей и цепочки хранения.

Таким образом, мы сталкиваемся с парадоксом: метаданные, являясь ключевым источником информации, не имеют соответствующего правового обеспечения.

Основная часть. Термин «метаданные» происходит от греческой приставки «мета-» (μετά), означающей «о», «над», «после», а в философском контексте – «о самом предмете». В сочетании со словом «данные» (data) термин приобретает смысл «данные о данных».

Во многих зарубежных и отечественных стандартах даются определения разных видов метаданных. Например, метаданные – это данные о данных; для файловых систем метаданные – это данные, которые предоставляют информацию о содержимом файла [5. С. 4-9]; метаданные файла – это атрибуты файла, определяемые прикладным программным обеспечением [1. С. 4].

Для целей цифровой криминалистики можно предложить следующее определение: «метаданные – это технически фиксируемые сведения о цифровом объекте, его происхождении, состоянии, использовании и взаимодействии, которые, не являясь его смысловым содержанием, образуют цифровой след, позволяющий установить хронологию событий, местоположение участников, идентифицировать технические устройства и доказать факт взаимодействия с информацией в целях раскрытия, расследования и предупреждения преступлений».

В условиях цифровой трансформации правоохранительной деятельности криминалистика сталкивается с необходимостью переосмысления традиционных категорий доказывания. Важнейшей задачей становится выстраивание четкой иерархической модели, которая бы последовательно связывала первичные данные, объекты исследования и процессуальные доказательства. Предлагаемая модель включает три взаимосвязанных понятия: метаданные, цифровой след и цифровое доказательство.

Метаданные представляют собой первичные цифровые данные, которые фиксируются автоматически техническими системами в процессе функционирования устройств и сетей. Как отмечает М.Р. Когаловский, «метаданные объекта ИТ – это представленное с помощью какого-либо выразительного средства описание или фрагмент объекта, характеризующие его свойства. Фрагменты объекта, используемые как его метаданные, выполняют функции идентификации этого объекта» [2. С. 20]. Метаданные не являются доказательствами по умолчанию, но служат фундаментальными строительными блоками для формирования более сложных структур. К метаданным относятся сведения о времени, месте, устройстве, IP-адресе, типе файла и других технических параметрах, которые не несут смыслового содержания, но характеризуют контекст взаимодействия.

Из метаданных, а также из содержательной информации (текст сообщения, содержание файла) и контекстных данных (история сессий, настройки системы) формируется цифровой след. Цифровой след – это комплексный объект, который характеризует факт взаимодействия пользователя с информационной средой и служит предметом криминалистического исследования. По своей функции он является аналогом традиционного физического следа (например, отпечатка пальца), но существует в виртуальной среде. В терминологии, используемой в форензике, подобные объекты часто называют «артефактами». Однако в контексте уголовного процесса более корректным является понятие «цифровой след», поскольку оно соответствует категории «вещественных доказательств» и интегрировано в правовую систему.

Наконец, цифровое доказательство – это цифровой след, который прошел процессуальную фиксацию (изъятие носителя, его осмотр, судебная экспертиза) и был признан судом в качестве допустимого доказательства. Оно возникает только в рамках уголовного процесса после соблюдения всех требований Уголовно-процессуального кодекса РФ. Ключевым условием его допустимости является документирование всех этапов обращения с доказательством, что в международной практике известно как цепочка хранения (chain of custody) [5. С. 2-8, 3-4, 4-7].

Таким образом, путь от технической информации до юридического доказательства проходит три этапа: от метаданных как исходных данных – к цифровому следу как объекту исследования – и, наконец, к цифровому доказательству как результату процессуального признания. Эта иерархия позволяет систематизировать работу с цифровой информацией и обосновать необходимость введения указанных понятий в российское законодательство.

В научной и профессиональной литературе, а также в законодательстве разных стран, часто упоминаются и используются термины «цифровое доказательство» (digital evidence) и «электронное доказательство» (electronic evidence) [4. С. 17]. Эти понятия близки по смыслу, но отражают разные правовые и технологические парадигмы; при этом ни одно из них не закреплено в Уголовно-процессуальном кодексе Российской Федерации, что порождает терминологическую неопределенность и затрудняет использование цифровых данных в качестве доказательств.

В российском уголовно-процессуальном законодательстве метаданные прямо не упоминаются. Однако на практике они используются как составляющая вещественных доказательств (ст. 83 УПК РФ), как результаты оперативно-розыскных мероприятий (ст. 6 Федерального закона от 12.08.1995 №144-ФЗ «Об оперативно-розыскной деятельности») и как материалы судебной компьютерно-технической экспертизы (ст. 204 УПК РФ). Проблема заключается не только в отсутствии нормативного закрепления их статуса, но и в недостатке единых криминалистических стандартов (правил) их фиксации, хранения и оценки, что приводит к спорам об их допустимости и достоверности.

Для того чтобы метаданные могли быть признаны доказательством, необходимо понимать, какие именно данные могут быть извлечены при их экспертном исследовании и как они формируются в ходе повседневной цифровой активности конкретных пользователей цифровых устройств.

Цифровая активность пользователя представляет собой совокупность разнообразных взаимодействий с устройствами, программными системами и сетевыми ресурсами. Каждое из таких взаимодействий сопровождается автоматической фиксацией технических параметров, которые и образуют метаданные. Эти данные несут в себе информацию не о содержании действия (например, тексте сообщения), а о самом факте взаимодействия, его контексте и условиях. Именно совокупность этих характеристик формирует цифровой след, который становится объектом криминалистического исследования.

В зависимости от типа активности, метаданные могут фиксировать различные технические параметры. В таблице 1 приведены основные категории цифровых взаимодействий и соответствующие им метаданные, которые могут быть использованы в ходе расследования преступлений.

Таблица 1

Примеры метаданных в зависимости от типа цифровой активности

Тип цифровой активности	Примеры метаданных
Взаимодействие с устройством	– время включения/выключения устройства – история запуска приложений – состояние батареи, версия ОС
Общение (мессенджеры, почта)	– время отправки/получения сообщения – IP-адрес отправителя – устройство (модель, ОС) – статус «онлайн»/«оффлайн»
Доступ к интернету	– время подключения к Wi-Fi/мобильной сети – MAC-адрес роутера – вышка связи (Cell ID) – список посещенных сайтов
Работа с файлами	– дата создания, изменения, копирования файла – автор файла (в свойствах документа) – путь к файлу на диске – хэш-сумма (SHA-256, MD5)
Геолокационная активность	– GPS-координаты при съемке фото – маршрут передвижения (Timeline) – время пребывания в точке
Аутентификация и вход в систему	– время входа в аккаунт – IP-адрес, с которого выполнен вход – устройство (User-Agent) – неудачные попытки входа

Анализ этих метаданных позволяет следователю восстановить полную картину происходившего: установить хронологию событий, определить местоположение участников, идентифицировать использованные устройства и доказать факт взаимодействия с информацией. Таким образом, технические характеристики цифровых взаимодействий являются ключевым элементом для формирования достоверного и юридически значимого цифрового доказательства.

Как показано в таблице 1, различные формы цифровой активности сопровождаются характерными метаданными, которые фиксируют технические параметры взаимодействий. Однако для того, чтобы эти данные приобрели статус доказательства, они должны быть объективно зафиксированы в рамках уголовного процесса. Это достигается путем включения сведений о метаданных в официальные документы, такие как протоколы следственных действий, заключения экспертов и материалы оперативно-розыскных мероприятий. Ниже приведены примеры, иллюстрирующие, как метаданные, подобные тем, что перечислены в таблице, фиксируются в практике работы правоохранительных органов.

Пример 1: Протокол осмотра телефона.

«При осмотре смартфона Samsung Galaxy S23 (IMEI: 352123456789012) установлено:

– время в системе: 15:23:10 (UTC+3), синхронизировано с сервером Google;

– в папке "DCIM" обнаружено 12 фото. EXIF-данные фото IMG_001.jpg: дата съемки – 10.08.2025 14:15:33, GPS-координаты – 55.7558° N, 49.1234° E, модель камеры – Samsung Galaxy S23.

Смартфон изъят и упакован в сумку Фарадея для предотвращения удаленного доступа. Упаковка опечатана наклейкой с указанием даты, времени, ФИО следователя и понятых. Хэш-сумма (SHA-256) резервной копии: a1b2c3d4...».

Пример 2: Заключение эксперта.

«С использованием Cellebrite UFED извлечены метаданные из личного чата Telegram пользователя +7 (917) XXX-XX-XX с абонентом +7 (927) XXX-XX-XX. Установлено:

– сообщение «Встреча отменяется» отправлено 05.08.2025 в 22:14:05;

– IP-адрес отправителя: 94.123.45.67 (ООО «Таттелеком»);

– устройство: Android 14, модель SM-G991 (смартфон Samsung Galaxy S22 Ultra);

– данные не подвергались модификации после отправки».

Пример 3: Материалы ОРМ

«На основании постановления о проведении ОРМ получены телеком-метаданные от ПАО «МегаФон».

Абонент +7 (927) XXX-XX-XX:

– 12.08.2025 в 18:05 – звонок на номер +7 (937) XXX-XX-XX (длительность 4 мин.).

– подключение к сети зафиксировано в период с 10.08.2025 по 15.08.2025.

– последнее подключение: 15.08.2025 в 10:30 к вышке связи № 1123 (Cell ID: 45678, LAC: 12345) – район ул. Петербургская, Казань (Местоположение абонента определено по данным о подключении к базовой станции (BTS ID: 1123), расположенной в районе ул. Петербургская, Казань)».

Эти примеры показывают, как первичные метаданные, выявленные в ходе технического анализа, трансформируются в юридически значимые сведения через процессуальную фиксацию. Именно в этот момент цифровой след, сформированный из метаданных, в соответствии с требованиями УПК РФ, приобретает статус процессуального доказательства и включается в совокупность доказательств по уголовному делу.

Несмотря на высокую доказательную ценность, использование метаданных в уголовном процессе сопряжено с рядом серьезных проблем. Одной из главных является отсутствие единых стандартов их фиксации при осмотре и изъятии электронных носителей. На практике следователи часто ограничиваются фиксацией только содержания файлов, не уделяя должного внимания метаданным, что делает доказательства уязвимыми к оспариванию в суде. Кроме того, метаданные подвержены фальсификации: с помощью специализированных инструментов, напри-

мер, программы ExifTool, можно изменить дату создания файла, геолокацию или IP-адрес, что затрудняет установление подлинности информации.

Еще одной существенной проблемой является процедурная ограниченность. Получение телеком-метаданных (например, данных о вышках связи, истории звонков, IP-адресах и точках подключения к сети) возможно только в рамках оперативно-розыскных мероприятий, что требует вынесения дополнительных постановлений и замедляет ход расследования. Кроме того, суды зачастую недооценивают метаданные, если они не подкреплены другими доказательствами, что связано с недостаточной цифровой грамотностью участников процесса и отсутствием в Уголовно-процессуальном кодексе РФ четкого определения их статуса.

Для преодоления этих и иных подобных проблем необходимо разработать единую правовую концепцию, включающую четкое разграничение понятий. Прежде всего, следует закрепить в УПК РФ понятие «цифровое доказательство» как самостоятельного вида доказательства, аналогично вещественным. Второе понятие – «цифровой след» – должно рассматриваться как следовой объект, включающий как содержательную информацию, так и метаданные, и являющийся предметом криминалистического исследования. Наконец, «метаданные» следует определить как составляющую часть цифрового следа, характеризующую его временные, пространственные и технические параметры.

Такой подход позволит избежать искусственного противопоставления и создать систему, в которой метаданные будут оцениваться как неотъемлемая часть доказательственной базы. Также необходимо разработать единые методические рекомендации по фиксации метаданных, включающие обязательное документирование хэш-сумм, правильное изъятие и упаковку электронных носителей, и детальное описание всех этапов работы с цифровыми доказательствами.

Заключение. Метаданные – это не просто дополнительная информация, а неотъемлемая составляющая цифрового следа, который, в свою очередь, формирует цифровое доказательство. Однако их потенциал до сих пор используется не в полной мере из-за правовых пробелов в российском уголовно-процессуальном законодательстве, недостатка специализированных знаний у участников процесса и отсутствия единых критериев оценки достоверности цифровых следов. Только комплексный подход – нормативное закрепление правового статуса цифровых следов (и в том числе, метаданных), внедрение единых стандартов по работе с ними, а также повышение цифровой грамотности сотрудников правоохранительных органов позволит превратить метаданные из «невидимой улики» в полноценное доказательство в уголовном процессе.

Список литературы

1. ГОСТ Р 57429-2017 «Судебная компьютерно-техническая экспертиза. Термины и определения».

2. Когаловский М.Р. Метаданные, их свойства, функции, классификация и средства представления (слайды доклада) // XIV Всероссийская научная конфе-

ренция RCDL-2012. Переславль-Залесский, 15-18 октября 2012 г. URL: http://www.rcdl2007.pereslavl.ru/doc/2012/ru.html (дата обращения: 07.09.2025).

3. Хомяков Э.Г. О сущности цифровых следов в криминалистике и их фиксации // Общество, право, государственность: ретроспектива и перспектива. 2025. №. 1. С. 71-82.

4. Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / отв. ред. С.В. Зуев. Москва: Юрайт, 2024. 193 с. (Высшее образование). Текст: электронный // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/543683 (дата обращения: 07.09.2025).

5. NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response. URL: https://csrc.nist.gov/pubs/sp/800/86/final (дата обращения: 07.09.2025).

УДК 341.482

К. В. Шевелева,
доцент кафедры,
Российский технологический университет – МИРЭА

О дополнительных мерах противодействия противоправным деяниям, совершенным с использованием информационных технологий

Аннотация. Раскрытие и расследование преступлений, совершаемых в цифровой среде, осложняется применением преступниками специализированных технических средств – в частности, электронно-вычислительных систем и современных информационно-коммуникационных технологий, интегрированных в архитектуру глобальной сети Интернет. Указанные обстоятельства создают существенные методологические и оперативно-технические трудности для следственных органов, затрудняя своевременное выявление, фиксацию и анализ доказательственной базы. Для преодоления данных барьеров целесообразно внедрение в следственную практику передовых информационных технологий, включая технологии искусственного интеллекта, понимаемого как программно-алгоритмический комплекс, предназначенный для автономного решения специализированных задач на основе обработки больших массивов данных без прямого участия человека. Обосновывается необходимость разработки формализованных алгоритмов взаимодействия следователей с ИИ-системами как дополнительной меры противодействия преступлениям.

Ключевые слова: уголовное право, преступление, цифровизация, искусственный интеллект, способ совершения преступлений, цифровые технологии, цифровые преступления

K. V. Sheveleva,
Associate Professor,
Russian Technological University – MIREA, Moscow, Russia,

On additional measures to counter unlawful acts committed using information technologies

Abstract. The detection and investigation of crimes committed in the digital environment is complicated by the use of specialized technical means by criminals, in particular, electronic computing systems and modern information and communication technologies integrated into the architecture of the global Internet. These circumstances create significant methodological and operational-technical difficulties for investigative bodies, complicating the timely identification, recording and analysis of the evidence base. To overcome these barriers, it is advisable to introduce advanced information technologies into investigative practice, including artificial intelligence technologies, understood as a software and algorithmic complex designed to autonomously solve specialized problems based on the processing of large amounts of data without direct human participation. This study substantiates the need to develop for-

malized algorithms for the interaction of investigators with AI systems as an additional measure to combat crime.

Key words: criminal law, crime, digitalization, artificial intelligence, method of committing crimes, digital technologies, digital crimes

Введение. В контексте цифровизации общественной жизни, актуализация проблематики уголовно-правового противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, приобретает первостепенное значение. Эволюция цифровых технологий обусловила расширение арсенала преступных методов, включая использование сети «Интернет» и иных цифровых платформ, для осуществления различного вида мошенничеств, кибертерроризма, кибершпионажа, распространения противоправной информации и объектов, ограниченных, либо запрещенных к обороту на территории Российской Федерации и др. преступлений. Указанное представляет угрозу не только для личной безопасности граждан, но и для стратегической стабильности и национальной безопасности Российской Федерации. Эскалация подобных правонарушений подчеркивает насущную потребность в постоянном аналитическом мониторинге современных тенденций киберпреступности, совершенствовании методов их пресечения и профилактики, а также в разработке технических решений, способных качественно повысить эффективность борьбы с преступностью.

Основная часть. Анализ данных за период с 2018 по 2024 год показывает статистически значимый тренд на увеличение инцидентов, связанных с киберпреступностью, с применением информационно-коммуникационных технологий. В течение указанного шестилетнего периода зафиксировано возрастание абсолютного числа таких преступлений с 174 674 до 676 951 случаев, что демонстрирует рост на 287,5% [3]. Это указывает на почти четырехкратное увеличение объема киберпреступлений, что подчеркивает нарастающую тревожность данной тенденции в контексте глобализации информационных технологий.

Вместе с тем, параллельно с увеличением числа преступлений, совершаемых при помощи информационно-телекоммуникационных технологий, коэффициент раскрытия таких преступлений остается на относительно низком уровне: 25.3% в 2021 году, снижение до 19.7% в 2022 году и незначительный рост до 21% в 2023 году. Это указывает на актуальность разработки и внедрения усовершенствованных методов противодействия преступлениям, совершаемым с использованием информационных технологий.

Статистика свидетельствует о том, что современное правовое поле сталкивается с необходимостью адаптации существующих механизмов противодействия преступлениям в сфере информационно-телекоммуникационных технологий, а также разработкой новых подходов, учитывающих специфику киберугроз.

Обозначенное обусловило цель настоящего исследования – анализ современных тенденций в развитии киберпреступности, выявление недостатков действующих методов противодействия им, а также обоснование перспективных направлений формирования комплексной стратегии борьбы с киберпреступлениями.

В свою очередь, под киберпреступлениями понимаем противоправные деяния, совершаемые посредством информационно-телекоммуникационных технологий, включая компьютерные сети, программные обеспечения, сеть «Интернет», приносящие вред интересам личности, общества и государства.

При этом отметим, что в настоящее время, практически любое преступление может осуществляться вышеуказанным способом, что подчеркивает особую остроту проблемы. Наиболее часто киберпреступления совершаются следующими способами: хакерская деятельность, несанкционированный доступ к информации, фишинг, фарминг, мошенничества методом социальной инженерии, кибертерроризм, киберсексуальные преступления, кибершпионаж и др.

Особую сложность представляют гибридные формы киберпреступлений, сочетающие элементы различных видов уголовных деяний, в ходе совершения которых преступники используют новейшие технологии искусственного интеллект.

Нельзя не отметить, что эффективность традиционных методов борьбы с киберпреступностью ограничена рядом объективных факторов.

1. Технологическая динамика: скорость развития технологий значительно опережает нормотворческий процесс. Многие положения законодательства, направленные на защиту от посягательств, не учитывают современные цифровые угрозы.

2. Трансграничный характер преступлений: границы киберпространства зачастую выходят за границы отдельного государства, что позволяет осуществлять преступления из любой точки мира. Это создает трудности в расследовании, выдаче запросов, сборе доказательственной информации и привлечении к ответственности лиц, находящихся за пределами страны.

3. Недостаточная осведомленность и подготовка кадров правоохранительной системы: современные вызовы предполагают владение не только умениями и навыками в сфере базовой юриспруденции, но и компетенциями в области информационных технологий. Образовательная подготовка таких сотрудников ведется лишь на нескольких кафедрах в Российской Федерации, что не покрывает кадровые запросы правоохранительных ведомств.

С учетом изложенного использование технологий искусственного интеллекта открывает новые возможности для борьбы с преступностью. Кроме того, «правоприменение по уголовным делам не может осуществляться в автоматизированном режиме без участия следователей. Поэтому возникает ряд принципиально новых задач организации их взаимодействия с искусственным интеллектом, а точнее, такого построения алгоритмов компьютерных программ данного вида, которое полностью укладывается в рамки уголовного и уголовно-процессуального законодательства» [1].

Современные алгоритмы позволяют эффективно анализировать большие объемы данных, выявлять скрытые закономерности и предсказывать поведение субъектов преступлений.

Наиболее интересными в контексте применения технологий искусственного интеллекта являются следующие направления.

1. Прогнозирование и аналитика поведения преступных лиц.

Прогностические модели на основе самообучаемых систем способны предсказывать места и время возможных преступлений на основании статистических сведений, материалов уголовных дел, криминальной обстановки, а равно текущих тенденций. Такие системы успешно реализуются в некоторых странах, например, система PredPol, разработанная в США. Программное обеспечение используется для прогнозирования места совершения преступления, лиц, осуществляющих преступную деятельность (включая прогнозирование развития криминальной «карьеры»), лиц, потенциально могущих стать жертвой преступления. Там активно используются так называемые «тепловые карты преступности» [4], которые не только показывают прошлые события, но и используя модели прогнозирования, указывают на наиболее вероятные места совершения следующих преступлений. С точки зрения разработки стратегии охраны правопорядка и планирования мест патрулирования, такого рода новеллы заслуживают всяческого внимания.

2. Биометрический контроль.

Использование биометрических данных уже в достаточной мере вошло в общественный обиход. Биометрия является важным инструментом идентификации личности. При этом сама биометрическая информация не ограничивается лишь уникальными, индивидуальными биологическими и физиологическими характеристиками человека, которые используются для его идентификации и аутентификации. В настоящее время к ним относятся отпечатки пальцев, изображение лица, голос, радужная оболочка глаза и другие характеристики, которые можно измерить и использовать для подтверждения личности. Однако и некоторые другие физиологические характеристики человека обладают свойствами индивидуальности, достаточности и относительной устойчивостью. Например, венозный рисунок пальцев рук, идентификация по которому – одно из самых интересных и многообещающих направлений в области криминалистики. Технологии распознавания вен пальца основаны на биологической особенности человеческого организма: способности гемоглобина крови поглощать инфракрасное излучение. В оборудовании применяется методика считывания отраженного инфракрасного излучения, основанная на алгоритмах машинного обучения. Сканер формирует изображение пальца с темным рисунком вен на нем. Система обрабатывает картинку и анализирует расположение кровеносных сосудов, а затем сравнивает с данными, записанными в базу.

Помимо этого, системы биометрической идентификации на основе технологий искусственного интеллекта широко применимы в области распознавания лиц на видеозаписях. При этом внедрение биометрической системы распознавания лиц «Сфера» в АПК «Безопасный город» позволило применять видеозаписывающие устройства не только с целью фиксации, но и для целей идентификации личности. Вместе с тем существует проблема неверного отождествления личности системой, связанной и с качеством «картинки», и с ограниченной базой данной, а также с недостаточной технической составляющей.

Для решения проблемы, вызванной ошибками идентификации в системе распознавания лиц необходимо улучшить качество камер и обеспечить их пра-

вильную установку, использовать современные алгоритмы на базе искусственного интеллекта, а также комбинировать разные технологии распознавания, включая 3D-анализ и инфракрасные методы (термограмма). Термограмма лица помогает идентифицировать человека, фиксируя инфракрасное излучение, исходящее от поверхности кожи, что отражает уникальное распределение температуры на лице. Этот тепловой рисунок (термограмма) является биометрическим образом, который можно использовать для аутентификации и распознавания личности. Важно регулярно обновлять и поддерживать техническое снабжение системы, а также правильно настраивать режимы работы системы в зависимости от задач. Не менее значима подготовка и повышение квалификации операторов, которые способны корректно интерпретировать результаты и выявлять ошибки.

3. Автоматизация фиксации следственных действий.

Технологии искусственного интеллекта могут быть использованы для автоматизации рутинных процессов, таких как фиксация хода следственного осмотра посредством протоколирования. Посредством компьютерного зрения возможно анализировать видеозаписи с места производства следственного действия и текстуально описывать его ход, обстановку и действия всех участников процесса.

Несмотря на то, что технологии искусственного интеллекта представляют интерес для правоохранительных органов, их применение может столкнуться с правовыми и этическими проблемами. Массовое применение нейронных сетей может привести к нарушению права граждан на защиту личной информации.

Кроме того, если система ИИ принимает решение, которое приводит к неправомерному задержанию или обвинению лица, возникает вопрос о распределении ответственности: кто будет ее нести – разработчик, оператор/пользователь или сам искусственный интеллект? Отметим, что данной дискуссия является наиболее популярной и обсуждаемой в правовой науке.

Полагаем, что с целью обеспечения справедливости и доверия к технологиям, необходимо, чтобы решения, принимаемые искусственным интеллектом, были объяснимыми и поддающимися проверке.

Согласимся с мнением Е.В. Пучковой, о том, что «внедрение цифровых технологий и ИИ в систему правоохранительных органов должно идти на опережение современному преступному миру, а не внедряться по результатам результатом уже прошедших антиобщественных действий» [2].

Заключение. Искусственный интеллект применяется как для осуществления законной деятельности, так и для противоправной [5, 6]. Таким образом, использование технологий искусственного интеллекта в борьбе с преступностью имеет большой потенциал и может рассматриваться в контексте дополнительных мер противодействия преступлениям, совершаемым посредством информационно-телекоммуникационных технологий. Однако этот потенциал должен реализовываться в строгом соответствии с правовыми принципами и этико-моральными нормами. Только при условии баланса между инновациями и защитой фундаментальных прав человека возможно формирование безопасной цифровой среды.

Список литературы

1. Бычков В. В., Прорвич В. А. «Алгоритмы взаимодействия следователей с искусственным интеллектом в ходе раскрытия и расследования преступлений экстремистского характера, совершенных с использованием интернета» // Правопорядок: история, теория, практика. 2021. № 2 (29). С. 92-97.

2. Пучкова Е. В., Морозов Р. М. «Российский и зарубежный опыт использования искусственного интеллекта в деятельности правоохранительных органов» // Право и управление. 2025. №. 1. С. 337-341.

3. Состояние преступности в Российской Федерации. URL: https://мвд.рф (дата обращения: 18.02.2025).

4. Crimes Heat Map. URL: https://data.cityofchicago.org/Public-Safety/Crimes-Heat-Map/puji-t6xd (дата обращения: 29.06.2025).

5. 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.

6. Шутова А. А. Применение технологий искусственного интеллекта в сфере здравоохранения: уголовно-правовые девиации // Правопорядок: история, теория, практика. 2023. № 3(38). С. 92-100. DOI 10.47475/2311-696X-2023-38-3-92-100. EDN RKMSGE.